

**A PREDICTIVE SAFETY MANAGEMENT SYSTEM SOFTWARE
PACKAGE BASED ON THE CONTINUOUS HAZARD TRACKING
AND FAILURE PREDICTION METHODOLOGY**

YEAR 1 FINAL REPORT

December 1, 2002 to November 30, 2003

November 30, 2003

Principal Investigator: Rolando Quintana, Ph.D., P.E.

The University of Texas at El Paso

Department of Mechanical and Industrial Engineering

500 West University Drive

El Paso, Texas 79968-0521

NASA Grant Number: NAG10-331

Technical POC: Mr. Bhupendra Deliwala, Kennedy Space Center

Mr. Chris Pino, OP-AM

Acknowledgements

The NASA Predictive Safety research team is very grateful to Mr. Bob Deliwala for his support, guidance and vision on the paradigm of predictive safety engineering and management. Many safety professionals have graduated with Bachelor's and Master's degrees working as research assistants in the NASA Predictive Safety Laboratory, including a significant number of women and underrepresented minorities. Through this grant Javier Avalos (M.S., Summer 2003) and Rene Roldan (M.S., Summer 2003) have been supported. Mr. Chris Pino is also acknowledged for his support.

Executive Summary

The goal of this research was to integrate a previously validated and reliable predictive safety model, called Continuous Hazard Tracking and Failure Prediction Methodology (CHTFPM), into a software application. This led to the development of a predictive safety management information system (PSMIS). This means that the theory or principles of the CHTFPM were incorporated in a software package; hence, the PSMIS is also referred to as CHTFPM management information system (CHTFPM MIS). The purpose of the PSMIS is to reduce the time and manpower required to perform predictive safety studies as well as to facilitate the handling of enormous quantities of information involved in this type of studies. The CHTFPM theory encompasses the philosophy of looking at the concept of safety engineering from a new perspective: from a proactive, rather than a reactive, viewpoint. That is, corrective measures are taken before a problem occurs, instead of after it happened. That is why the CHTFPM is a predictive safety approach because it foresees or anticipates accidents, system failures and unacceptable risks; therefore, corrective action can be taken in order to prevent all these unwanted issues. Consequently, safety and reliability of systems or processes can be further improved by taking proactive and timely corrective actions.

Table of Contents

Acknowledgements	ii
Executive Summary	iii
List of Tables	ix
List of Figures.....	x
Chapter 1	1
1. INTRODUCTION	1
1.1 Problem Statement.....	2
1.2 Problem Description	3
1.3 Problem Classification.....	4
1.4 Rationale for Solving Problem.....	5
1.5 Industrial Scenarios Analyzed	6
1.6 Scope and Purpose of Research	9
1.7 Organization of the Project Report	10
Chapter 2	11
2. LITERATURE REVIEW	11
2.1 Introduction.....	11
2.2 System Safety.....	12
2.3 Hazard Analysis	13
2.3.1 Preliminary Hazard Analysis	13
2.3.2 Failure Mode and Effect Analysis	14

2.3.3 Barrier Analysis	15
2.4 Risk Analysis and Demerit Scheme.....	16
2.5 Predictive Safety	18
2.5.1 Predictive Safety Models	21
2.5.2 CHTFPM.....	24
2.5.2.1 Dendritic Construction.....	26
2.5.2.2 Safety Sampling	27
2.5.2.3 Safety Control Charts.....	28
2.6 Predictive Safety Software.....	32
2.6.1 Predictive Reliability and Statistical Software	33
2.6.2 Computerized Predictive Safety	37
2.6.2.1 Predictive Simulation Software	37
2.6.2.1.1 Similarities between the MADYMO and the CHTFPM MIS	38
2.6.2.1.2 Differences between the MADYMO and the CHTFPM MIS	39
2.6.2.2 Computer Safety Monitoring Software.....	40
2.6.2.2.1 Similarities between the DSS and the CHTFPM MIS.....	40
2.6.2.2.2 Differences between the DSS and the CHTFPM MIS.....	42
Chapter 3	43
3. PREDICTIVE SAFETY SOFTWARE COMPONENTS	43
3.1 Introduction.....	43
3.2 Flowchart Symbols	44
3.3 Overview of the CHTFPM Program Utilization.....	45

3.4 General Overview of the PSMIS	48
3.5 Dendritic Construction.....	54
3.6 Safety Sampling	59
3.6.1 Groups, Subgroups and Observations per Subgroup	61
3.6.2 Preliminary Sampling Plan	63
3.6.2.1 Sample Size for Statistical Significance	66
3.6.2.2 Establish Control Limits	67
3.6.2.3 PSMIS Process to Establish Control Limits	71
3.6.3 Actual Sampling Plan	73
3.6.4 Pareto Analysis	76
3.7 Safety Control Charts Theory	78
3.7.1 Control Chart for Nonconformities.....	79
3.7.2 Control Chart for Fraction Nonconforming.....	81
3.7.3 Control Chart for Average Nonconformities per Unit.....	82
3.7.4 Weighted Control Chart.....	84
3.7.5 EWMA Chart.....	86
3.7.6 Combined Shewhart—EWMA Control Chart.....	90
3.8 Decision Support Structure of the PSMIS	91
3.8.1 Management Reports of the PSMIS	94
3.8.2 Help Screens and Decision Support.....	97
Chapter 4	101
4. IMPLEMENTATION AND EVALUATION OF THE PSMIS.....	101

4.1 Introduction.....	101
4.2 Implementation and Evaluation Synopsis of the PSMIS	102
4.3 Development of Dendritic Elements.....	103
4.3.1 Preliminary Hazard Analysis	104
4.3.2 Failure Mode and Effect Analysis	106
4.3.3 Barrier Analysis	109
4.3.4 Dendritic Construction.....	110
4.4 Design of the Sampling Sheet.....	113
4.5 Rational Subgroups, Sample Size and Sampling Plan.....	117
4.6 Statistical Significance.....	119
4.7 Establish Control Limits and Control Charts.....	122
4.7.1 Control Charts for the MSFC Case Study.....	126
4.7.2 Control Charts for the KSC Case Study	137
4.8 Reliability and Efficiency of the PSMIS	141
4.8.1 Efficiency of the PSMIS in the MSFC Case Study	144
4.8.2 Efficiency of the PSMIS in the KSC Case Study	146
Chapter 5	149
5. CONCLUSIONS AND RECOMMENDATIONS	149
5.1 Introduction.....	149
5.2 Summary of Work Performed.....	149
5.3 Conclusions.....	151
5.4 Potential Implementation Problems.....	152

5.5 Future Research Recommendations.....	154
References	155
Glossary	162
APPENDIX A: Preliminary Hazard Analysis for the MSFC Project.....	167
APPENDIX B: Failure Mode and Effect Analysis for the MSFC Project.....	169
APPENDIX C: Barrier Analysis for the MSFC Project.....	173
APPENDIX D: c Control Chart Data for the MSFC Project.....	175
APPENDIX E: Weighted Control Chart Data for the MSFC Project.....	177
APPENDIX F: EWMA Control Chart Data for the MSFC Project ($\lambda = 0.4, L = 3.054$)	180
APPENDIX G: EWMA Control Chart Data for the MSFC Project ($\lambda = 0.1, L = 2.814$)	183
APPENDIX H: Preliminary Hazard Analysis for the KSC Project	186
APPENDIX I: Failure Mode and Effect Analysis for the KSC Project.....	190
APPENDIX J: Barrier Analysis for the KSC Project.....	196
APPENDIX K: Classification of Dendritics for the KSC Project.....	198
APPENDIX L: c Control Chart Data for the KSC Project	201
APPENDIX M: Weighted Control Chart Data for the KSC Project.....	203

List of Tables

Table 3.1: Techniques for dendritic construction (Quintana <i>et al.</i> , 2001).....	54
Table 3.2: Average run lengths for several EWMA control schemes (Lucas and Sacucci, 1990).	88
Table 3.3: Summary of control chart applications in the CHTFPM (Quintana <i>et al.</i> , 2001).....	98
Table 4.1: Classification of dendritics for the MSFC project.	130
Table 4.2: Summary of the efficiency elements for the MSFC project.	146
Table 4.3: Summary of the efficiency elements for the KSC project.	148

List of Figures

Figure 1.1: Cross section of the promoted combustion testing chamber	7
Figure 1.2: Joint airlock and HPGTs located in the cargo bay of the shuttle at KSC	8
Figure 2.1: Schematic of the CHTFPM (Quintana <i>et al.</i> , 2001)	25
Figure 3.1: Flowchart symbols and their meanings (Whitten <i>et al.</i> , 1989).....	44
Figure 3.2: Flowchart of the entire CHTFPM MIS general process	47
Figure 3.3: Schematic of the core events of the PSMIS.....	49
Figure 3.4: Main menu of the PSMIS.	49
Figure 3.5: “Delete a project” event of the PSMIS.	50
Figure 3.6: Delete window of the PSMIS.	50
Figure 3.7: “Exit program” event of the PSMIS.	51
Figure 3.8: Beginning portion of the “Create a new project” event of the PSMIS.	52
Figure 3.9: New project information screen.....	53
Figure 3.10: Message box indicating that a required field is empty.....	53
Figure 3.11: Dendritic construction process in the PSMIS.....	56
Figure 3.12: Edit feature for the dendritic list.....	57
Figure 3.13: Flowchart for assigning weights to dendritics.....	59
Figure 3.14: Flowchart of preliminary sampling plan.	65
Figure 3.15: Flowchart to calculate number of samples needed for statistical significance.....	68
Figure 3.16: Process that the PSMIS follows when the user estimates \hat{p}	70

Figure 3.17: Flowchart for the calculation of the control limits.	72
Figure 3.18: Flowchart of actual sampling plan.	75
Figure 3.19: Flowchart for calculating total dendritic frequency and entire chart values.	77
Figure 3.20: Assignable cause patterns on a control chart (Wise and Fair, 1998)	93
Figure 3.21: Flowchart of management reports (part 1).	95
Figure 3.22: Flowchart of management reports (part 2).	96
Figure 4.1: Comparison between the (a) manual and (b) PSMIS approach for the PHA forms of the MSPC case study.	104
Figure 4.2: Comparison between the (a) manual and (b) PSMIS approach for the PHA forms of the KSC case study.	105
Figure 4.3: Comparison between the (a) manual and (b) PSMIS approach for the FMEA forms of the MSFC case study.	107
Figure 4.4: Comparison between the (a) manual and (b) PSMIS approach for the FMEA forms of the KSC case study.	108
Figure 4.5: Comparison between the (a) manual and (b) PSMIS approach for the barrier analysis forms of the MSFC case study.	109
Figure 4.6: Comparison between the (a) manual and (b) PSMIS approach for the barrier analysis forms of the KSC case study.	110
Figure 4.7: Comparison between the (a) manual and (b) PSMIS dendritic list of the MSFC case study.	111

Figure 4.8: Comparison between the (a) manual and (b) PSMIS dendritic list of the KSC case study.	112
Figure 4.9: Sampling sheet created manually for the MSFC project.	113
Figure 4.10: Sampling sheet developed by the PSMIS for the MSFC project.	114
Figure 4.11: Sampling sheet created manually for the KSC project.	115
Figure 4.12: Sampling sheet developed by the PSMIS for the KSC project.	116
Figure 4.13: Preliminary sampling plan created by the PSMIS for the MSFC project.	118
Figure 4.14: Preliminary sampling plan created by the PSMIS for the KSC project. ..	119
Figure 4.15: Statistical significance screen for the MSFC project provided by the PSMIS.	120
Figure 4.16: Statistical significance screen for the KSC project provided by the PSMIS.	121
Figure 4.17: Screen for selecting the type of Shewhart chart control limits.	124
Figure 4.18: Control parameters of the c chart for the MSFC case study.	124
Figure 4.19: Control parameters of the c chart for the KSC case study.	125
Figure 4.20: MSFC project c chart, as constructed by the analyst.	126
Figure 4.21: MSFC project c chart, developed by the PSMIS.	127
Figure 4.22: MSFC project Pareto diagram, as constructed by the analyst.	128
Figure 4.23: MSFC project Pareto diagram, developed by the PSMIS.	129
Figure 4.24: MSFC project weighted chart, as constructed by the analyst.	131
Figure 4.25: MSFC project weighted chart, developed by the PSMIS.	132

Figure 4.26: MSFC project EWMA chart ($L = 3.054$ and $\lambda = 0.4$), as constructed by the analyst.....	133
Figure 4.27: MSFC project EWMA chart ($L = 3.054$ and $\lambda = 0.4$), developed by the PSMIS	133
Figure 4.28: MSFC project EWMA chart ($L = 2.814$ and $\lambda = 0.1$), as constructed by the analyst.....	134
Figure 4.29: MSFC project EWMA chart ($L = 2.814$ and $\lambda = 0.1$), developed by the PSMIS	135
Figure 4.30: MSFC project combined Shewhart-EWMA chart ($L = 2.814$ and $\lambda = 0.1$), as constructed by the analyst.	136
Figure 4.31: MSFC project combined Shewhart-EWMA chart ($L = 2.814$ and $\lambda = 0.1$), developed by the PSMIS.	136
Figure 4.32: KSC project c chart, as constructed by the analyst.	137
Figure 4.33: KSC project c chart, developed by the PSMIS.	138
Figure 4.34: KSC project Pareto diagram, as constructed by the analyst.....	138
Figure 4.35: KSC project Pareto diagram, developed by the PSMIS.....	139
Figure 4.36: KSC project weighted chart, as constructed by the analyst.	140
Figure 4.37: KSC project weighted chart, developed by the PSMIS.....	141

Chapter 1

1. INTRODUCTION

This chapter emphasizes the need to look at the concept of safety engineering from a new perspective: from a proactive, rather than a reactive, point of view. That is, remedial action should be taken before the fact, instead of after the fact, resulting in safer and more reliable systems or environments in the workplace. For this reason, predictive risk analyses have come into an increasing role in providing the most meaningful and useful information regarding system assessment and system safety (Cooper, 1998). A predictive safety model for prevention of accidents and system failures, called Continuous Hazard Tracking and Failure Prediction Methodology (CHTFPM), served as the foundation for the development of a predictive safety management information system (PSMIS). This research incorporates the CHTFPM into a software package with a system's safety decision support structure.

In Section 1.1, the problem is identified concerning the lack safety in industry. A description of the problem currently faced is given in Section 1.2. The classification of the problem is described in Section 1.3, followed by Section 1.4 which provides the rationale for investigating and solving the problem. Section 1.5 gives a brief overview of the case study scenario that was analyzed in order to test the PSMIS. In Section 1.6, the scope and purpose of the research is defined. At the end of this chapter, Section 1.7 delineates the organization of the project report.

1.1 Problem Statement

The presence of hazards in the work environment may cause numerous accidents which may lead to personnel injuries or system malfunctions; this happens due to lack of safety. Many work related injuries transpire in industry every year. A case in point, just in 1992, a total of 6.8 million injuries and illnesses were reported in private industry workplaces resulting in 60 million lost workdays, according to a survey by the Bureau of Labor Statistics, U.S. Department of Labor. Consequently, US employers incurred more than \$60 billion in direct workers' compensation costs in 1992 (Quintana *et al.*, 2001). In addition, counting costs such as production delays, damage to equipment, recruitment and training of replacement workers brought the total cost for the year to approximately \$350 billion (Olsen, 1993).

The Occupational Safety and Health Administration (OSHA) requires employers to provide safe and healthful working conditions for every working man and woman; this is a mandatory regulation under Public Law 91-596 which is officially known as the Occupational Safety and Health Act of 1970. However, the above facts demonstrate that there is a tremendous lack of safety in the workplace; therefore, there is still much room for improvement in the present system safety programs being used in industry today. That is why predictive safety is a key point to be included as part of a preventative safety programs in order to ameliorate or eliminate some of these expensive problems.

Additionally, not many studies in predictive safety are seen in the literature; thereby, there are not many existing predictive safety software products, but recently, there has been a considerably growth of predictive safety models. Nonetheless, such

models serve to conduct safety assessments from a reactive (after-the-fact) point of view but not from a predictive or proactive perspective; this means that accident causes are investigated after an incident has taken place to determine what must be done to predict and prevent similar situations.

1.2 Problem Description

Accidents or system malfunctions do not happen unless a hazard exists (Marshall, 1982). Thereby, the tracking of safety hazards is essential to predictive safety, but present system safety methods typically do not do this (Cooper, 1998). These safety programs are usually established piecemeal, based on an after-the-fact philosophy of accident prevention (Roland and Moriarity, 1983). As an illustration, when an accident or system malfunction occurs, an investigation is conducted to determine the causes. The relevant causes are then reviewed and discussed to determine what must be done to prevent similar accidents or malfunctions. Finally, the resulting system modifications or corrections of design safeguards or procedures are made to existing systems (Quintana *et al.*, 2001).

What is required is a method or an approach that indicates if the system under consideration is becoming hazardous; this information would help to check and eliminate the hazard before accidents can happen. The CHTFPM is an approach that alerts systems personnel of unsafe situations that could lead to mishaps. The CHTFPM is a new predictive safety concept which involves a planned, systematically organized, and before-the-fact process characterized as the identify-analyze-control method of safety. This

predictive safety model uses the principles of work sampling and control charts, the keys to track hazards (Quintana *et al.*, 2001).

In order to trace hazards, it is imperative to identify the core or unsafe conditions that can potentially originate them. These core conditions are the building blocks of hazards and can be termed dendritic elements. Dendrite is a word use by materials scientists to describe the microstructure of the building blocks of metals (Mangonon, 1999). The development or expansion of multiple dendrites is called dendritic growth, hence the term dendritic elements or simply dendritics. Thus, the dendritics form the basis for performing continuous safety sampling to evaluate whether the system is becoming hazardous, so that proactive actions can be taken to avoid accidents or system failures.

Besides the lack of predictive safety models that are proactive, these are not offered or do not exist in a software application. Therefore, the necessity for developing satisfactory analysis and predictive methods for software is extremely acute that much research, effort, and money continues to be spent (Davies *et al.*, 1987). There are, however, some statistical softwares that employ control charts to determine the stability of a process or system. Unfortunately, such computer programs do not include the predictive safety portion, which is the identification of dendritics—the building blocks of hazards—, and a self-contained, safety focused decision support structure.

1.3 Problem Classification

The problem described in Section 1.2 can be classified as a safety computer

system challenge, for an integrated safety software application is a project that is difficult because of the elaboration time it demands (Wrench, 1990). Furthermore, Wrench (1990) clarifies that the development of a safety management information system (MIS) requires sophisticated technology and design of databases, skilled programming, and software design experience. As a result, this kind of problem encompasses an elementary theme.

The fundamental subject is that the development of a safety software application must be a team effort. In addition, the team should be comprised of computer software professionals and safety professionals (Wrench, 1990), which is the pattern followed in this research. Two graduate students formed the project group; one is a computer science major and the other one is a manufacturing engineering major (specialized in safety engineering). The computer scientist focused on the design aspect of the software—structure, format, presentation, *etc.*—while the safety specialist contributed with the predictive safety part of the software, which is the main topic of this project.

1.4 Rationale for Solving Problem

The goal of this research was to make available the CHTFPM in an easy-to-use electronic MIS. This means that the theory behind the CHTFPM was integrated in a single computer program. The intent was that the PSMIS would carry out all computations automatically in order to facilitate to the user the planning, tracking, control, management and prediction germane to a system's safety project. Additionally, the safety status of a system can promptly be known. This signifies that the analyst has a rapid response to system changes because the user is seeing the effects of the system

almost immediately (Mackie, 1998). Moreover, faster preventative safety measures can be adopted, ensuing in a quicker elimination of the hazard.

It is evident that an integrated MIS approach offers many advantages over hand computations and even traditional computer programs, like Microsoft Excel, that helps in performing calculations and analyzing information. The aspect of this approach makes it easier to exercise control over the calculation processes (Mackie, 1998); furthermore, the most important benefit is the richer data handling capabilities that are available (Mackie, 2001). Even though the idea of incorporating the CHTFPM into a software packet sounds attractive, it is not a simple job. Designing a dependable software system that is able to deliver critical services with a high level of confidence is not an easy task (Kaâniche *et al.*, 2002), especially if there are not many predictive safety software applications available that can act as a benchmark. For this reason there is an urgent necessity of developing an integrating predictive safety management information system (PSMIS).

1.5 Industrial Scenarios Analyzed

The CHTFPM can be utilized in any industrial scenario in general since it is robust and, hence, is broadly applicable. To demonstrate the potential utility of the CHTFPM MIS, it will be tested using two previous predictive safety studies. One of the investigations was carried out at NASA Marshall Space Flight Center (MSFC) to analyze the promoted combustion testing chamber operations. The other one was done on the hoisting operation, testing and preparation of four high-pressure gas tanks (HPGTs) at NASA Kennedy Space Center (KSC).

The first preventative safety research was performed at the Material Combustion Research Facility located in MSFC where the system under scope was the promoted combustion testing chamber, depicted in Figure 1.1. Specimens were loaded into a promoted combustion testing chamber. Ordinarily, the test samples are 1/8-inch diameter, 12-inch rods of metal or alloy, although the chamber allows up to 18-inch rods.

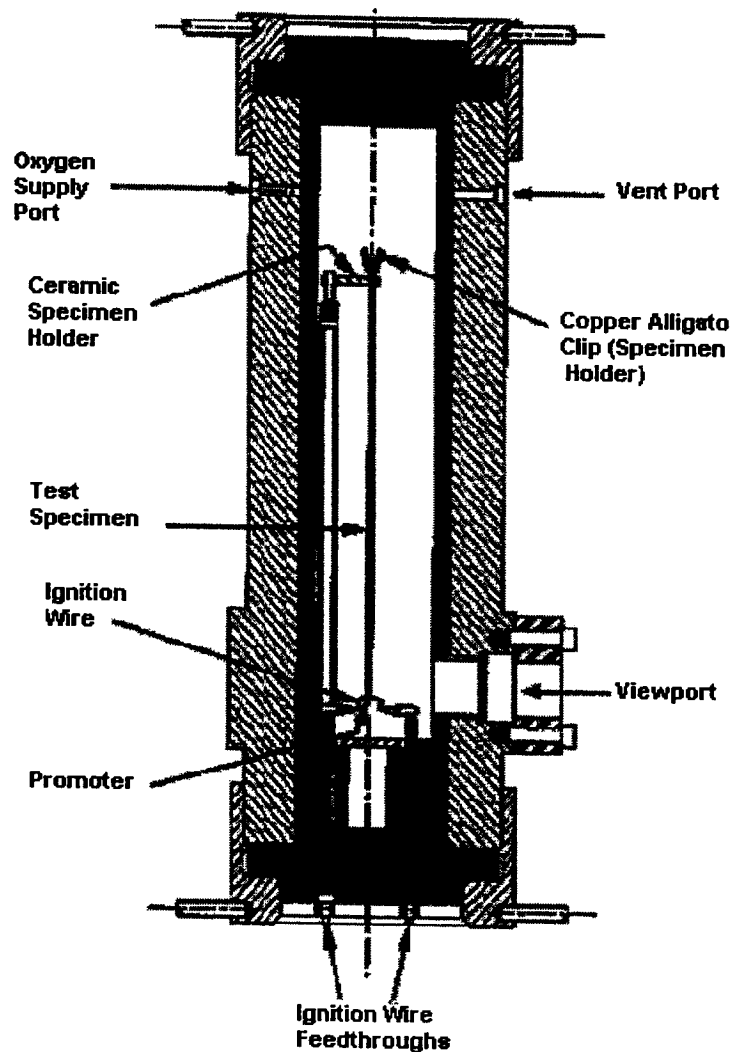


Figure 1: Cross section of the promoted combustion testing chamber.

After initial placement of the test sample into the promoted combustion chamber, an aluminum igniter is attached to the sample. The chamber is then filled with 100 percent gaseous oxygen (GOX) bringing the chamber up to the desired test pressure, a maximum of 10,000 pounds per square inch (psi) is allowed. The sample is ignited and allowed to burn. A carbon dioxide laser provides an alternate ignition method if so desired. After the samples were ignited, the burn length of each sample was recorded. A burn length of more than 6 inches on any one sample constitutes failure of the material.

The second proactive safety project is based on four gaseous tanks that were part of a shuttle mission. On July 12, 2001, NASA launched the space vehicle U.S. shuttle Atlantis: STS-104 mission with flight crew 7A aboard. The five-member crew would install a new joint airlock as well as two oxygen and two nitrogen gas storage tanks on the International Space Station (ISS). Figure 1.2 shows the joint airlock and the four HPGTs being loaded in the cargo bay of the Atlantis shuttle at KSC.

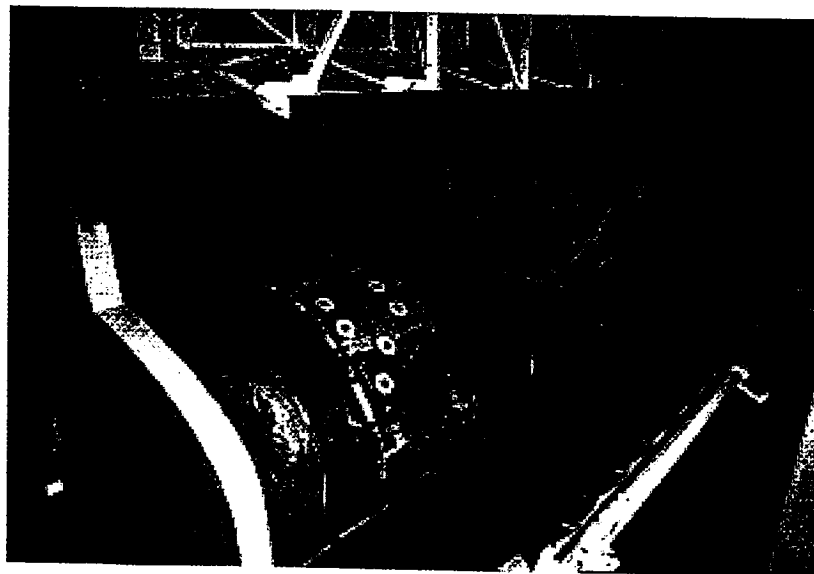


Figure 1.2: Joint airlock and HPGTs located in the cargo bay of the shuttle at KSC.

The new joint airlock would enable crews to perform space walks without the presence of a shuttle while recovering over 90 percent of the gases that were previously lost when airlocks were vented to the vacuum of space. The four high-pressure gas tanks (HPGTs) would serve to support future station experiments and space walks (<http://www.pao.ksc.nasa.gov/shuttle/summaries/sts104/index.htm>).

The HPGTs, were especially made by a private contractor and tested before being delivered to NASA KSC. In order to insure 100% reliability of each individual tank, the staff at KSC decided to again submit the four tanks under more rigorous tests on various aspects such as pressure and temperature limits, proper functioning of the tanks in general, *etc.* During these kinds of tests, the HPGTs had to be moved from one place to another within the same building with a hoist. Thus, the tanks had to be hoisted with extreme care in order to be displaced to different locations; that is why the hoisting operation was also a substantial aspect of this particular project.

1.6 Scope and Purpose of Research

The main objective of this research is to develop a computer program that will facilitate the lengthy and tedious process of predictive a safety management. This software system will have included the underlying theory of the CHTFPM. A secondary objective is to make the PSMIS an easy-to-use program, which implies that it must contain a friendly-user interface, so the analyst can navigate through the program in a simple manner. Another objective is that the CHTFPM MIS can provide the user with charts, diagrams and results that are quickly and accurately interpreted.

Coupled with the objectives previously stated, the goal of this study is to validate the performance of the PSMIS by testing it using the two case scenarios described previously. The efficiency of the software application will be determined mainly by the time and number of persons required to complete each research study without the aid of the CHTFPM MIS relative to when it was employed. Moreover, the same information collected pertaining to the studies expressed in Section 1.5 will be utilized in the CHTFPM MIS to observe if the same results are achieved, which have been previously validated.

1.7 Organization of the Project Report

This project report is partitioned in five chapters. Chapter 1 has been already explained, which introduced the current problem that is being faced and the approach that will be taken to solve such challenge. Chapter 2 gives a detailed review on the literature pertinent to predictive safety models as well as present software programs, along with their attributes associated with preventative safety. Chapter 3 describes all the components of both the CHTFPM theory and the PSMIS.

Chapter 4 depicts the implementation and evaluation of the PSMIS by comparing the results of the PSMIS with the ones obtained in the original studies and by showing the efficiency of the PSMIS in terms of time and manpower (persons) needed to finish the projects. Finally, Chapter 5 provides the conclusions and recommendations that will help for future research.

Chapter 2

2. LITERATURE REVIEW

This chapter consists of the literature pertaining to existing software associated with safety models and issues, such as predictive safety, hazard tracking and control charts. Specifically, the most pertinent subjects related to safety analysis will be covered, especially aspects in the work environment and industry. In addition, the concept of safety models that predict accidents will be studied; that is, safety methods that serve to prevent accidents or system failures before they occur.

2.1 Introduction

This chapter begins with a discussion of the concept of system safety in Section 2.2. Section 2.3 covers literature related to hazard analysis with its corresponding salient topics: PHA, FMEA and Barrier analysis. Section 2.4 describes the concept of risk analysis and risks classifications. In Section 2.5, the theory of predictive safety is discussed extensively with some predictive safety models as examples; this section, additionally, includes a description of the CHTFPM and its components—dendritic construction, work sampling and control charts. Finally, Section 2.6 provides information of existing computer predictive safety software.

2.2 System Safety

The presence of hazards in the work environment may cause numerous accidents which may lead to personnel injuries and system failures; this happens due to lack of safety. For this reason, safety is an essential consideration for all projects (Cheng *et al.*, 2002). System safety is an element of systems engineering involving the application of scientific and engineering principles for the timely identification and control of hazards within the system (Preyssl, 1995).

The safety of the employees and the customers is a principal factor in any process; that is why the use of system safety programs has grown considerably in the work environment. Thereby, many industries focus on the safety engineering aspect of their processes by employing methods and techniques to ensure the safety requirements for the system are met (Spalding, 1998). For instance, some companies implement in their facilities safety assessments as part of their system safety programs.

A safety assessment evaluates the safety of the project's output (typically systems or equipment). Assessments are aimed at providing confirmation or otherwise of the project's safety claims. Additionally, they provide evidence for the safety case and should be viewed as assistance to the project providing necessary confidence as to the integrity of the system (Spalding, 1998). A pertinent reason of why safety assessments are part of system safety programs is to assure that any system does not produce an intolerable degree of risk. There are many different types of safety assessment techniques that assist in identifying hazardous conditions and risks becoming intolerable; some of the most commonly known practices are hazard analyses and risk analyses.

2.3 Hazard Analysis

According to Lee *et al.* (1998), new hazards do arise: they must be identified, the risks assessed and managed. Hazard identification should be used at each stage of any development or process. In some cases, as the procedure advances in an operation, more detailed assessment of hazard have to be performed. Once recognized, by an ongoing or periodic process of review and reporting, the systems personnel must assess the risks arising from the hazards (Lee *et al.*, 1998). Wherever achievable, hazards should be eliminated. Nevertheless, where this is not possible, then the primary means of risk reduction is to ameliorate the likelihood of the hazard occurring or to minimize the severity of the accident. There must be a systematic identification and analysis of hazards related to the system (Spalding, 1998). Thereupon, the following techniques are essential steps in a hazard analysis:

1. Preliminary Hazard Analysis (PHA).
2. Failure Mode and Effect Analysis (FMEA).
3. Barrier Analysis.

2.3.1 Preliminary Hazard Analysis

A preliminary hazard analysis (PHA) or hazard identification is a systematic, creative examination of a process or function performed to traverse a representation of the parts of the system and their interactions (Spalding, 1998), either with other components or the operators. PHA provides an initial risk assessment of a system,

identifies safety critical areas, evaluates hazards, and identifies the safety design criteria to be used (Grimaldi and Simonds, 1989). The PHA effort should thus commence during the initial phases of system development, or in the case of a fully operational system, at the initiation of a safety evaluation (Quintana *et al.*, 2001).

In this stage of the investigation, the system is analyzed at the top level to derive a list of hazards that might be exhibited. Hazard identification is typically carried out using brainstorming, checklists and/or hazard study techniques. It is also imperative for credibility that the assessor has the appropriate expertise to assess the project technically.

Thereafter, the evaluator considers the process intention of each component in turn and by applying a list of guided words attempts to reveal plausible deviations or anomalies from the process purpose (Spalding, 1998). The hazards associated with the proposed design or function are identified and evaluated for potential hazard severity, probability, time of exposure, and hazard classification (Quintana *et al.*, 2001). As a consequence, engineering and/or administrative controls as well as other measures deemed necessary to eradicate or decrease unsafe conditions to a tolerable degree should be contemplated and recorded.

2.3.2 Failure Mode and Effect Analysis

This phase of the procedure analyzes the system at more detailed levels to derive the cause-effect chains that could lead to the hazards. The failure mode and effect analysis (FMEA) is a common technique employed in causal analysis in order to determine the credible combinations or sequences of causal factors which can lead to

hazardous situations. The FMEA requires a hierarchical breakdown of the system's structure of functionality (Spalding, 1998).

If a possible risk continues unnoticed by the PHA, the FMEA should help in detecting it. FMEA provides further analysis at the lowest level for hazards identified in the PHA and can even identify hazards caused by failures that may have been previously overlooked by the PHA. With FMEA, the analyst chooses a level of the hierarchy to start at, considers components or issues at a detailed level of the hierarchy and records their failure modes along with causes and effects in tabular form (British Standards Institution [BSI], 1991). The failure effects of these subcomponents then become failure modes of components at the next higher level. The procedure may be repeated to yield the individual failure modes of the entire system (Spalding, 1998).

2.3.3 Barrier Analysis

At this step of the process, the trace of a threat that could lead to an accident is analyzed. A barrier analysis is utilized to determine the condition and final consequences arising from the identified hazards (Spalding, 1998). In addition, a barrier analysis looks at these potential sources of problems or hazards as well as how the harm or damage occurred (Wilson *et al.*, 1993). Moreover, it also examines any root cause of the problem or unwanted event by assessing the adequacy of any installed barriers or safeguards that should have prevented, or at least mitigated, its occurrence (Quintana *et al.*, 2001).

Barrier analysis defines the basic elements of an undesirable event or problem as the following (Wilson *et al.*, 1993):

1. The threat or hazard that does the harm
2. The people or thing (target) that is harmed
3. The barrier(s) that could have or should have prevented the threat from reaching the target
4. The path or trace by which the threat reached the target

There are two kinds of barriers: paper barriers and physical barriers. Paper barriers may be procedures—norms, standards, rules, etc.—that should be followed when performing a task. On the other hand, physical barriers may be material objects—special tools, safeguards, protective equipment, etc.—that serve as an obstacle to prevent the operator from reaching or going into an unwanted location. It is evident from the diversity of barriers available for restraining a threat that some barriers will be more successful than others in providing protection against hazards.

2.4 Risk Analysis and Demerit Scheme

A risk analysis may be performed quantitatively, qualitatively or comparatively according to the information available. In any case, the purpose of a risk analysis is to ascertain whether or not the risk has been reduced to a tolerable level or whether further activities are recommended to minimize it further (Spalding, 1998). The risk levels of safety systems are described in the legal framework set out by the Health and Safety Executive (HSE) in 1992 as follows:

1. Intolerable risks. These are risks that are not acceptable under any circumstances.
2. Negligible risks. These are risks that have been reduced to such a low level that no

further precautions are deemed necessary; the risks is acceptable as is stands.

3. Tolerable risks. These are risks that fall between the two previous categories, where the risk is acceptable as long as it has been decreased to the lowest level practicable, bearing in mind the benefits flowing from its acceptance and taking into account the costs of further reduction.

Put in another way, the different types of risks can be further classified into more specific categories or classes according to the acuteness of the defect. Furthermore, one of the objectives of the risk analysis is to quantify uncertainty and to apply a severity factor to it (Kaplan, 1991).

To quantify uncertainty, a numerical scale is established which is called frequency distribution. A frequency distribution reflects the variability of a parameter over a population. In principle, a frequency distribution is measurable by sampling the population (Montgomery, 1996).

Severity refers to the impact of loss in terms of destroyed product, loss in dollars, damaged equipment/machinery, or degree of physical impairment (Kaplan, 1991). In addition, severity may be time dependent, it may be uncertain, or it may be both time dependent and uncertain. Using the factors of frequency and severity, a risk analysis develops classes of severity and frequency; these classes are used to rank the relative risk of various events. In this research project, a demerit scheme divided in four classes was employed to classify the dendritics according to their severity. The demerit scheme used in this study was the same as the one recommended by Montgomery (1996), which is the following:

1. Class “A” defects – Very serious. This type of defect will render the unit unfit for service. It will surely cause operating failure of the unit in service that cannot be readily correct on the job and is liable to cause personal injury or property damage.
2. Class “B” defects – Serious. This defect will probably, but not surely, cause a *Class A* operating failure of the unit in service. It will cause trouble of a nature less than *Class A* operating failures and will cause increased maintenance or decreased life.
3. Class “C” defects – Moderately serious. A Class C defect could possibly cause operating failure of the unit in-service and is likely to cause trouble of a nature less serious than operating failure as well as increased maintenance or decreased life.
4. Class “D” defects – Not serious. This defect will not cause operating failure of the unit in service but does account for minor defects of appearance, finish, or workmanship. This type of defect accounts for major defects of appearance, finish, or workmanship.

Once all defects or nonconformities are established, they can be grouped in such a way as to accurately portray the seriousness of a defect when compared to others. By categorizing the nonconformities (dendritics) into classes, the necessary corrections can be better directed to the dendritics that require immediate attention, according to their severity.

2.5 Predictive Safety

Regarding predictive safety studies, there has not been much research directed

towards predictive safety, but many parallels to predictive safety can be drawn from the subject of predictive maintenance or predictive reliability. The escalating operation and maintenance costs of modern manufacturing processes have caused a search for ways to reduce costs while maintaining a high level of safety and reliability (Johnson, 1995). A predictive maintenance program is a tool that addresses this problem—sustaining safety and reliability at a low cost—and has become widely accepted throughout industry (Shreve, 1996). Additionally, the concept of measuring or foreseeing the failure of a machine component is the central idea of predictive maintenance.

Under a predictive maintenance program, conditions that cause loss of function or impaired performance of a component or system are identified and monitored. Hence, a corrective action plan can be carried out in the case that these conditions are occurring, thereby limiting actual in-service failures or failures to operate on demand (Johnson, 1995). In order to apply predictive maintenance to a structure, system, or component, the failure modes and mechanism associated with these entities must be identified and understood. This information is essential to ensure that the proper conditions are being monitored for effective maintenance (Chelbi and Ait-Kadi, 1998).

Just as in predictive maintenance, a predictive safety program must also identify the failure modes and mechanisms associated with system failures. The different failure modes and mechanisms that need to be identified are the building blocks of hazards; these building blocks of hazards are called dendritic elements. Dendrite is a term use by materials scientists to describe the microstructure building blocks of metals (Mangonon, 1999). The development or expansion of multiple dendrites is called dendritic growth,

hence the name dendritic elements or simply dendritics.

In an effort to implement an analogy, the materials science term dendrite (dendritic) is employed in predictive safety to represent the cornerstone of hazards. More exactly, the dendritics recognize the initial cause that gives birth to a hazard. That is why dendritics are essential factors in forecasting safety studies because they assist in identifying hazards; subsequently, they can be eliminated before taking place. Further, hazard and risk analyses act as powerful tools in recognizing these dendritics in a system, which may lead to a hazard; more important, the tracking of safety hazards is essential to predictive safety (Quintana *et al.*, 2001). The relationship between these two investigations is that risks arise from hazards; that is, a hazard imports a level of risk.

Once recognized, by an ongoing or periodic process of review and reporting, risks arising from the hazards can be assessed. Furthermore, corrective action can be taken in order to prevent any risk before occurring. In other words, these tools alert systems personnel of unwanted situations; therefore, these safety approaches aid in predicting system failures or accidents. This means that the risk, thus the probability of an accident, imported by a hazard can be prevented before occurring, resulting in a predictive and preventive safety action.

Zissler (1996) notes that after a failure impact is determined, there must be a means to quantify or measure parameters that will indicate the hazardous condition of the equipment being monitored. However, choosing which parameters to measure is often the difficult portion of implementing the predictive safety program (Chelbi and Ait-Kadi, 1998). These parameters are discerned by constantly monitoring the system for the

occurrence of specified conditions or dendritics which in return could lead to hazards or unacceptable risks. Once the parameters are chosen, the questions of how, when and where to take such readings must be addressed and determined; all these points provide the information required to commence the predictive safety plan.

2.5.1 Predictive Safety Models

As was pointed out earlier, a modest amount of research is found in the literature on predictive safety issues. However, these types of studies have been gradually increasing in the last couple of years since they are a potent, cost-effective tool. Predictive risk (safety) analyses have come into an increasing role in providing the most meaningful and regarding system assessment and system safety (Cooper, 1998). An advantage of predictive safety models is that they are applicable to many case scenarios and are thus robust.

For instance, the implementation of these predictive safety analyses may include, but not limited to: issues in chemical/nuclear plants, environmental issues, traffic incidents and not to mention industrial/manufacturing process. These steadily-rising models contain similar characteristics which serve to obtain a common goal, predict accidents, yet some of this methods lack in one or more fundamental elements of the prediction aspect.

For instance, accident prediction models for urban junctions and road links were developed recently and presented in an article named "Accident prediction models for urban roads" (Greibe, 2002). Such models are explained in "Uheldsmodel for bygader-

Del1: Modeller for 3-og 4-benede kryds. Notat 22, The Danish Road Directorate” (Greibe and Hemdorff, 1995) and “Uheldsmodel for bygader-Del2: Modeller for strækninger. Notat 59, The Danish Road Directorate” (Greibe and Hemdorff, 1998).

The main objective of these models is to predict the expected number of accidents at urban junctions and road links as accurate as possible. In order to develop the models, detailed information on accident data, traffic flow and road design was collected from the official accident statistics database covering all police recorded accidents (Greibe, 2002). These models used information that was previously recorded for estimating accident prediction.

This kind of data acquisition demonstrates that the data employed in the calculations were not current, and thus did not provide up-to-the-minute results. Moreover, these accident prediction programs take a reactive, instead of a proactive, approach to predict or prevent similar anomalies. In other words, when an accident arises, an investigation is conducted to determine the causes. The relevant causes are then reviewed and discussed to determine what needs to be done to prevent similar accidents.

These safety programs are usually established piecemeal, based on an after-the-fact philosophy of accident prevention (Roland and Moriarity, 1983). The tracking of safety hazards is essential to predictive safety, and present system safety methods typically do not do this (Cooper, 1998). In addition, these models did not employ control charts, the keys for predictive safety (Quintana *et al.*, 2001), to determine if the roads were operating under the presence of hazards.

Another example of a predictive safety method is a safety monitoring model which evaluated the performance of road programs. This model was described in a published paper labeled "Monitoring performance of road programmes in New Zealand" (Guria and Mara, 2000). Such approach was based on developing a control chart system to identify the occurrence of actual risk changes or deviation from the expected level. In addition, these control charts were utilized to monitor fatalities. Unlike the previous models described, this one employed new real time data to perform the analysis. The data was incorporated in the control charts to identify the risk changes, so that necessary measures could be undertaken.

Nonetheless, an inconvenience of this model is that charts can be developed on monthly or weekly basis. Monthly charts have an advantage of a longer period of time during which the random ups and downs are smoothed; this issue is particularly important for fatalities. However, a disadvantage is that it takes a long period of time to get an indication of any risk changes. Weekly charts, on the other hand, have the disadvantage of short time period. A crash with relatively large number of deaths indicates occurrence of an unexpected phenomenon while its occurrence is possible due to randomness. This needs to be taken into consideration while interpreting the charts.

An advantage of the weekly chart, relative to the monthly chart, is that within a few weeks it provides an indication of any risks changes. However, although this monitoring safety model utilizes up to date information and control charts to spot any variations in road safety, it still has the disadvantage of not giving descriptive safety statistics of a system on a daily basis. This means that a considerably amount of time has

to pass by in order to obtain any valuable insight on the safety status of a system, even when weekly charts are used.

Therefore, a more complete and reliable predictive safety model that has been developed, entitled Continuous Hazard Tracking and Failure Prediction Methodology (CHTFPM), will be employed in this research because it addresses the lacking traits of existing predictive safety models. Some missing attributes of present anticipatory safety models which are met by the CHTFPM are utilizing real-time or current data, making use of control charts to determine the safety status of the system, and providing those diagrams almost immediately, even on a daily basis. Moreover, the CHTFPM predicts accidents and systems failures before they reach the user or affect the system.

2.5.2 CHTFPM

The Continuous Hazard Tracking and Failure Prediction Methodology (CHTFPM) is a predictive safety model. It involves a process that is well planned, systematically organized, and before-the-fact and which is characterized as the identify-analyze-control method of safety (Quintana *et al.*, 2001). This methodology looks at the concept of safety from a proactive, rather than a reactive, perspective; that is, remedial action is taken before the fact, instead of after the fact. The way the model achieves the previous objective is by tracking a system for the occurrence of conditions becoming unsafe. Then it alerts safety managers or systems personnel of the hazardous conditions previous to happening; therefore, corrective action can be taken before the risks activate, hence, resulting in a proactive safety measure.

As was mentioned in Section 2.5, the dendritics have to be defined prior to the implementation of the predictive safety plan, in this case the CHTFPM. Spotting the proper dendritics is critical for implementing an effective CHTFPM. The CHTFPM utilizes established system safety tools as the ones mentioned in Section 2.3—PHA, FMEA and barrier analysis—for detecting the dendritics. The CHTFPM relies heavily on these methods for an initial risk assessment of the system and subsequent breakdown and analysis of system hazards to determine what the building blocks, or dendritics, of the associated hazards are. The dendritics form the foundation for using the CHTFPM to determine whether the system is becoming hazardous. Figure 2.1 shows the CHTFPM plan.

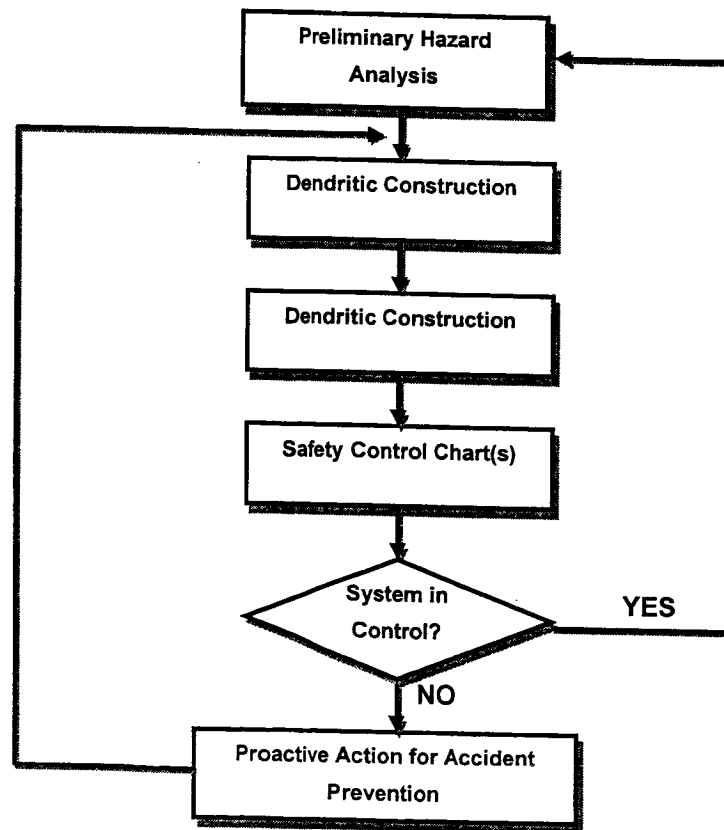


Figure 2.1: Schematic of the CHTFPM (Quintana *et al.*, 2001).

It is important to emphasize that the effectiveness of the CHTFPM depends on the identification of the dendritics; these building blocks of hazards are use for performing the sampling study of a given system. In addition to the identification of dendritic elements, the CHTFPM utilizes concepts underlying the predictive approach to system which are derived from work sampling and control chart theories, the keys to tracking hazards (Quintana *et al.*, 2001).

2.5.2.1 Dendritic Construction

As was explained in Section 2.5, the dendritics have to be defined first in order to implement the CHTFPM. Recognizing the proper dendritics is critical for implementing an effective CHTFPM. Many of these dendritics or defects emerge due to human error. According to Marcombe (1993), accidents-injuries and the disruption of scheduled system operation caused by human element factors shows that the human element is a very significant factor affecting the safety of systems. Unfortunately, many system predictive methods are based solely on equipment failures neglecting the human interaction of man-machine systems (Koval, 1997). Therefore, it is enormously vital for credibility that the analyst has the appropriate expertise to assess the project not only technically but also taking into consideration the human interaction with the system.

The CHTFPM employs the previously described PHA, FMEA and barrier analysis, for detecting the dendritics; that is, the CHTFPM strongly relies on these techniques for dendritic construction. The reason why the CHTFPM uses these approaches is because they can be applied to human factors analysis. Defining unsafe

behavior of operators is important when considering overall system safety. When constructing the dendritics for a given system, the human interaction with the system cannot be ignored and must be included (Camet, 1999).

The way the CHTFPM elaborates a list of dendritics is by analyzing and reviewing with detail each entry of the PHA, FMEA and barrier analysis. Afterwards, a preliminary dendritic list is formed by choosing the items that will lead to possible occurrences which could result in system failure or employee injury—sometimes the human is considered as the system. Finally, the initial dendritic record is double-checked for any repeating or similar elements and to enhance the wording of the items, ensuing in the concluding version of the dendritic list. Nevertheless, the final list of dendritics can be modified if more defects or hazardous conditions are found since undetected or new hazards may arise. As indicated by Lee *et al.* (1998), sometimes as the procedure advances in an operation, more detailed assessment of hazards has to be performed.

2.5.2.2 Safety Sampling

Safety sampling or work sampling is originated from probability conditions. A work sampling investigation consists of a number of random observations taken at different intervals in time. CHTFPM utilizes the principles of monitoring, trending and pattern recognition to draw inferences. The CHTFPM model emphasizes the application of work sampling theory in order to prevent undue risks and accidents. According to Meister (1985), accidents are preventable. This prevention is hardly attained and is achieved by employing an immense amount of effort conducting periodic, thorough

inspections and vigilance on the part of operations supervisors. Nonetheless, avoidance of unwanted, grave situations can be less difficult if work sampling and control charts, taking advantage of the dendritics list, supplement safety inspections.

The CHTFPM conducts work sampling in a random fashion, rather than at fixed periods of time, which is the way safety inspections are performed. Moreover, work sampling is used in the CHTFPM as a plain way to present a measure of the tendency of the system in a productive and cost-effective manner. Just as work sampling is used to give a measurement of over-all performance, the sampling in CHTFPM gives an over-all view of the safety status of the system under observation (Camet, 1999). If the system exhibits symptoms of becoming harmful, then effective control measures can be carried to preserve a desired degree of safety; hence, resulting in prevention of an undesirable, severe consequence.

2.5.2.3 Safety Control Charts

The core of the CHTFPM is to monitor the system to identify the dendritics that lead to hazards. The control charts incorporate these dendritics into graphs to indicate if the system is out of control when the system is operating under the presence of these defects. In the predictive safety model CHTFPM, control charts are used to measure the tendency of a system when is becoming hazardous. After sampling is performed, a control chart is constructed graphically by means of a characteristic that has been measured or computed, with a predetermined level of safety.

The chart contains a center line that represents the average value of the quality characteristic corresponding to the in-control state (Montgomery, 1996). Two outer horizontal lines called the upper control limit (UCL) and the lower control limit (LCL) are also shown on the charts. These control limits are chosen so that if the system is in control, nearly all of the sample points will fall between them. If no points go outside the bands, it is not necessary to take corrective action. On the contrary, if a point is outside the bands or limits, it means that a hazard is present or that the system is out of control, requires immediate attention. Thus, the control charts are powerful instruments for stabilizing and controlling the system or process at desired operability levels. The advantages of control chart applications in industry are listed as follows (Montgomery, 1996):

1. Control charts are a proven technique for improving productivity. Just as control charts improve productivity, they are used to improve the safety status of a given system in the CHTFPM. The control chart provides the technique to evaluate system safety as well as measure the success of corrective actions.
2. Control charts are effective in defect prevention. The control charts utilized by the CHTFPM are effective in hazard prevention. By detecting the conditions that lead to hazards, dendritics, the control chart provides the impetus to act and correct the conditions before hazardous conditions or unacceptable risks occur.
3. Control charts prevent unnecessary process adjustment. The control charts in the CHTFPM indicate when corrective actions need to be taken, by indicating out-of-control situations, thus preventing unnecessary system adjustments.

4. Control charts provide diagnostic information. Analysis of the control charts in the CHTFPM can yield information on the safety status of the system under observation. By indicating when the system went out-of-control, the control chart actually directs the efforts of the system analyst in investigating the causes of accidents or system malfunctions.
5. Control charts provide information about process capability. The control charts in the CHTFPM provide an overall view of system safety and give a good indication of the relative degree of safety that the system possesses.

The control charts described previously are usually called Shewhart control charts, as they are based on the principles of control charts developed by Dr. Walter A. Shewhart (Montgomery, 1996). The signal that the process may be out of control, ignoring the use of runs testing, is the occurrence of a single point outside the 3σ limits (Hunter, 1986). Even though Shewhart control charts have many advantages, they are relative insensitive to small shifts in the process, on the order of about 1.5σ or less (Ryan, 1989).

That is why one alternative to the Shewhart control chart may be used when small shifts in the process are of interest: the exponentially weighted moving average (EWMA) control chart (Hunter, 1986). The performance of the EWMA control chart is, in some ways, easier to set up and operate. The EWMA control chart can be viewed as a method for establishing real-time dynamic control of the process being monitored (Hunter, 1986). The EWMA control chart can be used in CHTFPM when the risks of not detecting small shifts in the safety mean of the system under observation rise to unacceptable levels.

As mentioned earlier, the EWMA performs well detecting small shifts but does not react to large shifts as quickly as the Shewhart control chart. A good way to further improve the sensitivity of the control procedure to large shifts without sacrificing the ability to detect small shifts quickly is to combine a Shewhart control chart with the EWMA (Borror *et al.*, 1998). These combined Shewhart-EWMA control procedures are effective against both large and small shifts. It is also possible to plot both the Shewhart chart and the EWMA chart on the same chart along with the associated control limits for each chart (Hunter, 1986). The use of either the Shewhart control charts or the EWMA control chart, or both, in CHTFPM depends upon the nature of the system being analyzed and the desired protection from risks and unacceptable hazards. The EWMA control chart as well as the different kinds of Shewhart control charts and the associated equations for their construction will be discussed in further detail in Chapter 3.

Besides the utilization of control charts, the Pareto analysis is a useful tool in knowing which dendritics required immediate attention. The relationship between these two techniques is that the control chart indicates if there is reason to suspect that the system may be becoming hazardous with respect to the sampled dendritics; consequently, this result provides the rationale to carry out a more comprehensive study of individual dendritic occurrences using Pareto analysis. This will provide an indication about which one of the dendritics has the highest frequency of occurrence; thus necessary and proactive measures can be taken more specifically for accident prevention.

2.6 Predictive Safety Software

With the rapid evolution of technology, there is a swift increase and development of computer software. This proliferation of software has emerged in almost any area and field of study there is: medicine, science, engineering, etc. The aim and scope of this section consists of the literature concerning existing software associated with predictive safety. To be more precise, only the most relevant topics related to preventative safety analysis will be covered. In addition, the concept of safety models that intent to predict accidents will be studied; that is, safety methods that serve to prevent accidents or system failures, especially in an electronic or automatic manner, before they occur.

The purpose of this project is to integrate the CHTFPM in a computer software package. That is, the intent of this study is to use the underlying theory of the CHTFPM described in all the previous sections of this chapter in a single, simple electronic management information system (MIS). The intended predictive safety software will carry out all computations and will provide the user (analyst or assessor) the adequate graphs such as Pareto diagrams or control charts, as requested. By this means, the safety status of the system under consideration will be quickly available; with this attribute, a greater degree of interaction with the software can be achieved. This is especially true in the area of rapid response to system changes because the user is seeing the effects of the system almost immediately, and thereby, a greater level of interaction being released (Mackie, 1998). Furthermore, faster preventative safety measures can be adopted, giving as a result an earlier cancellation of the hazard.

2.6.1 Predictive Reliability and Statistical Software

Not many studies in predictive safety are seen in the literature; thereby, there are not many existing predictive safety software products. Most of the available safety computer systems serve to conduct safety assessments from a reactive (after-the-fact) point of view but not from a predictive or proactive perspective. Lately, there has been a considerably growth of predictive safety models; nonetheless, such models—as the ones revealed in Section 2.5.1—are not offered in a software package. Therefore, the necessity for developing satisfactory analysis and predictive methods for software is so acute that much research, effort, and money, continues to be spent (Davies *et al.*, 1987).

In addition, evoking from Section 2.5, predictive safety can be drawn in parallel from the subject of predictive maintenance or predictive reliability. In this topic, there are several software applications, such as Alvey and Esprit programmes; additionally, Proportional Hazard Modeling methods for software reliability data were largely developed (Davies *et al.*, 1987). For predictive reliability software, in particular, analyst have focused upon these methods as a systematic approach to the incorporation of the wealth of supplementary information often available in software development or software reliability databases (Davies *et al.*, 1987). Some early work in this area was undertaken by Boeing in the USA (Nagel and Skrivan, 1981) and continuing interest was followed in France (Font, 1985); moreover, Wightman and Bendell (1986) were the ones to apply Proportional Hazards modeling to reliability software.

At the beginning of the 1980's, a typical software reliability prediction method required data comprising a history of the times at which individual failures occurred

(Dale and Foster, 1987). This typical quality, similar to the predictive models elucidated in Section 2.5.1, manifests that such reliability predictive methods needed information that was previously recorded for estimating failure prediction. This mode of data acquisition demonstrates that the data employed in the calculations was not current, which is preferable so that more modern results can be obtained, leading to more accurate deductions. Likewise, these reliability prediction programs also adopted a reactive, instead of a proactive, approach to foresee similar system breakdowns. As per Roland and Moriarty (1983), these safety (reliability) programs are usually established piecemeal, based on an after-the-fact philosophy of accident prevention. In order to be proactive, the tracking of safety hazards is essential to predictive safety, and present system safety methods typically do not do this (Cooper, 1998), including predictive safety computer applications.

Another major feature in the 70's and early 80's of reliability software was the incorporation of statistical models proposed for assessment and prediction (Veevers *et al.*, 1987). However, some approaches back then carried a heavy computational burden, and hence statistical methods were not readily implementable for software applications; even more, this state of affairs reflected the fact that no software reliability model was generally useful or applicable (Veevers *et al.*, 1987). The difficult interpretation by the non-statistician and the inappropriateness of the predictive statistical methods for software applications were mainly due to the fact that in the past this type of software did not have a user-friendly interface such as a Windows environment. The CHTFPM software addresses and meets these issues—data presented in an easy-to-understand

manner and generally applicable to different case studies. In present times, incorporation of statistical methods in software reliability prediction is feasible (Veevers *et al.*, 1987); in fact, various statistical software packages, like MINITAB, DATAPAC, *etc.*, are available for statistical analysis of data including virtually all types of control charts.

Today's statistical software can calculate the sample parameters, initial control limits and control charts. Most software can provide additional summaries and analyses such as listings of the raw data, out-of-specifications values, histograms, checks for runs and other patterns within control limits, tests for normality, process capability calculations, Pareto analyses, and trend analyses (Juran, 1988). Unfortunately, such software programs are only for statistical purposes and do not take into account the safety aspects of a project, especially the human interaction portion. In the words of Koval (1997), many reliability or statistical predictive methods are based solely on equipment failures neglecting the human interaction of man-machine systems. This signifies that the statistical programs do not typically provide dendritic identification capabilities.

Furthermore, the safety information would have to be stored by the analyst in a different location from the statistical program, either on paper or electronically. Therefore, in a predictive safety study, safety data would have to be first stored in one location (database, paper files, *etc.*) and then extracted from its original site and input again in the statistical software for calculations. This reflects that the inputting of data has to be done twice which, apart from interaction inefficiencies, could lead to possible mistakes (misinterpretation or human error) at the time of re-entering the data, resulting in erroneous conclusions.

The CHTFPM software will comprise the safety and statistical aspects together in one, single software application; this implies that the safety information will be saved in the same program where the statistical computations will be executed. To be more precise, safety records and/or reports will be kept in a database contained in the CHTFPM computer program. Getting information out of the records, however, is a cause of frequent frustration, which is why professionals need to look critically at their recordkeeping practices from gathering data to providing information (Wrench, 1990). It is strongly recommended, therefore, to use databases to store safety records and/or information.

That is why Wrench (1990) urges each health and safety professional to calculate on an annual basis the cost in time to produce every record in the office, the cost of the space the records occupy, the cost of the cabinets and shelves they fill, and the cost of the time spent in trying to find data when needed. An examination of this sort can be revealing since the cost is likely to equal or surpass the cost of the personnel hired to ensure company health and safety. If this lesson were taken to heart, controls would be instituted and an immediate effort would be made to computerize. Moreover, by having safety reports together with the statistical portion in the same software package, records will not have to be re-entered, thus, no faults due to human error will be exhibited. In fact, the reckonings will be carried out automatically after the safety data has been recorded.

Besides keeping safety records outside the statistical computer system, current statistical software products do not offer the user suggestions or recommendations for

performing calculations. For instance, the analyst may try to use a p chart to analyze some data; however, such information is best represented by a c chart. Consequently, the results may not be accurate, leading to false conclusions or wrong interpretations. The CHTFPM will also tackle this limitation; it will supply to the assessor the suggestions and options of what type of analyses are more adequately suited for the data collected, according to the circumstances of the system under observation.

2.6.2 Computerized Predictive Safety

In conjunction with predictive reliability and statistical software, there exist simulation methods and computer aided safety monitoring whose foci are linked to predictive safety. These computer approaches monitor systems and analyze collected data to identify possible causes of adverse or hazardous conditions. Thus, prediction of anomalies and concomitant appropriate actions can be taken to prevent system failures and accidents. Some existing computerized safety monitoring and prediction systems are like the CHTFPM software application in various aspects. The similarities and differences between these computerized methodologies and the CHTFPM computer program are discussed in this section.

2.6.2.1 Predictive Simulation Software

In a traffic accident prediction study, injury potential of a safety design feature is predicted by using laboratory/mathematical simulation data of traffic accidents (Norin

and Isaksson-Hellman, 1995). The research states that mathematical simulations could predict by correlation the type of injuries in a certain accident configuration before the system is exposed to harmful circumstances (in this investigation the human was the system). In this report, MADYMO mathematical simulation software models (TNO, 1990) are used. The MADYMO simulation models were validated for Volvo 240 cars from full scale crashes at several speeds and from a Hyge sled test series (Norin *et al.*, 1991). This computer/mathematical simulation method has several similarities to the CHTFPM software program.

2.6.2.1.1 Similarities between the MADYMO and the CHTFPM MIS

The first similarity of MADYMO with the CHTFPM MIS is that such approach is proactive, which means that it can predict accident likelihood (in this case risk injuries) in advance, hence, influence the design and manufacturing of the vehicle before a mishap reaches the user. As indicated by the article, the purpose of this method is to create a means of predicting to what extent a component of a car can influence the risk of injury before the system is exposed to real traffic conditions. By paying particular attention to such components, corrective action can take place before the driver is exposed to hazards (Norin and Isaksson-Hellman, 1995).

A second similarity this computer simulation model has with the CHTFPM electronic version is that it can be generalized or applicable for other protection systems and for other accident types (Norin and Isaksson-Hellman, 1995). A third likeness is that the mathematical safety simulation approach, just as the computerized CHTFPM, utilizes

a large amount of current information collected in new real-time from the experiments to perform calculations. This indicates that data from preceding or previous accidents was not employed—instead, in-progress data was used—to predict accidents.

A fourth similarity between the two compared models is that both take into account the human interaction with the machines. In the case of the MADYMO simulation methodology, the machine is the car, and the human interaction parameters considered are occupant size, seating position, among others. (Norin and Isaksson-Hellman, 1995). A functioning of a system must consider the human-system where the humans are involved with it (Bologna and Hollnagel, 2002). The person's behavior has to be defined and quantified when considering overall system safety.

2.6.2.1.2 Differences between the MADYMO and the CHTFPM MIS

Just as this method has similarities to the CHTFPM MIS, it also has dissimilarities. Unlike the CHTFPM computer system which displays control charts, the MADYMO application only provides distribution graphs to make inferences about the safety standing of the system.

Another difference there is between the two is that the mathematical MADYMO model always implies a simplified description of reality and certain faults (errors) occur with such generalization (Norin and Isaksson-Hellman, 1995). This denotes that such software does not quantify possible error of the results, whereas the CHTFPM program does.

2.6.2.2 Computer Safety Monitoring Software

An additional safety software application is a safety monitoring computer program that measures adverse conditions in the system requiring attention; thus, such unacceptable situations can be addressed and solved before resulting in an accident. A construction report written by Cheng *et al.* (2002) focuses on describing the development of a decision support system (DSS) for safety monitoring of excavations in construction sites. This computer system is designed to assist construction engineers in monitoring and controlling the excavation conditions that could become hazardous with the aid of instruments (wall inclinometer, strut and rebar strain gages, *etc.*) placed in the construction field. Like the previously depicted computer simulation system (MADYMO), the DSS also has various analogous aspects to the CHTFPM MIS.

2.6.2.2.1 Similarities between the DSS and the CHTFPM MIS

One identical feature to the CHTFPM MIS is that the DSS is a before-the-fact safety technique, which implies that its predictive aspect prevents accidents due to the fact that corrective action can take place before they can occur. As sustained in the articles, predictions of adverse conditions and appropriate actions can be taken to prevent construction accidents (Cheng *et al.*, 2002). Another equal attribute the DSS has with respect to the CHTFPM computer software is that it utilizes present-day information, gathered from the instruments located in the construction field, to perform computations which entail the safety state of the system.

An additional characteristic of the DSS is that it helps identify possible causes and origins of hazardous conditions (Cheng *et al.*, 2002). This is an analogy of the FMEA and dendritic qualities, respectively, of the CHTFPM software application. More exactly, the possible causes of adverse conditions in the DSS resemble the causes of the failure modes depicted in an FMEA (which is enclosed in the CHTFPM computer program). In the same way, the possible origins of unacceptable situations in the DSS are analogous to the dendritics (building blocks of hazards) in the CHTFPM software package.

One more comparable element between the DSS and the CHTFPM software program is that both employ databases to store safety information in the same application where the reckonings are realized. The use of databases is highly recommended since it facilitates data handling/management. In effect, by applying open database connectivity, the program data interface writes/reads the information to/from the associated databases, respectively. Moreover, through this process, the stored safety data files can act as the communication media (Cheng *et al.*, 2002).

A final, similar mark to the CHTFPM MIS is that the DSS is a PC-based software program. The prime development tools of the DSS include Visual Basic, MS Excel, Access and MapInfo, which were developed in a Windows environment. Further, the user communicates with the system components through a custom interface developed with Visual Basic (Cheng *et al.*, 2002). All the previously defined points are also part of the CHTFPM software, including the use of Access as a platform. Additionally, just like the computerized CHTFPM, the DSS—when compared with manual methods—significantly

improves automation in safety monitoring, enhances computational efficiency and increases data accuracy and consistency (Cheng *et al.*, 2002).

2.6.2.2.2 Differences between the DSS and the CHTFPM MIS

In the same manner the MADYMO computer simulation system has some distinctions from the CHTFPM software, the DSS computer program differs from the CHTFPM MIS as well. For example, an obvious dissimilarity is that the DSS does not use control charts as the source for portraying the system's safety status. The DSS, rather, displays graphical trends as well as data distribution plots that depict the safety degree of the scheme and estimates possible accident likelihood.

In addition to not utilizing control charts, the DSS differs from the CHTFPM software packet because the first method is not generally applicable, while the CHTFPM MIS is robust. Although the DSS is applicable within the subject of construction work, it is inappropriate for other case scenarios since it requires special equipment or instrumentation absolutely used in construction.

The last difference between the DSS and the computerized CHTFPM is that the DSS is costly to use. The electronic CHTFPM, however, is a cost-effective tool because it does not require any additional allocation of resources (Quintana *et al.*, 2001). The DSS, on the other hand, collects and transmits measured data from the construction ground to the job site office using automated transmission technology through cable connections or wireless communication. Therefore, this factor, besides the measuring instruments, contributes to a high cost to implement such a safety monitoring system.

Chapter 3

3. PREDICTIVE SAFETY SOFTWARE COMPONENTS

The focal point of this study is to incorporate the theory behind the CHTFPM into a software package; therefore, this chapter describes the CHTFPM constituents both in theory and in the computer program. First, an overview of the ingredients of this predictive safety model will be explained in order to understand how the predictive safety management information system (PSMIS) will work. Subsequently, the integration of the CHTFPM elements into a programmable system will be depicted in the form of flowcharts to portray the functioning of the CHTFPM MIS.

3.1 Introduction

This chapter exposes in Section 3.2 the flowchart symbols used in the program design of the PSMIS as well as their meaning. In Section 3.3, an overview of the entire program utilization is provided, followed by general overview of the software package in Section 3.4. The construction of dendritics is explained in Section 3.5. Section 3.6 talks about the preliminary samples needed to establish control limits. Control chart theory is presented in Section 3.7. Section 3.8, describes the topics related to safety sampling. In Section 3.9, the Pareto analysis is elucidated. Finally, Section 3.10 consists of the help and decision support offered to the user.

3.2 Flowchart Symbols

Before revealing the CHTFPM components in theory as well as in a flowchart fashion, it is essential to understand the meaning of symbols employed in the diagrams that show how the MIS will carry out a certain process or task. A reason for choosing flowcharts to explain the process of the predictive safety computer system is because program design frequently involves the use of flowcharts (Whitten *et al.*, 1989). In addition, system flowcharts were one of the very first tools commonly used by systems analysts and computer programmers.

The American National Standards Institute (ANSI) has established certain symbols that have been widely used in the computer industry to describe the logic of both systems and computer programs (Whitten *et al.*, 1989). The symbols that were utilized in the flowcharts for the development of the PSMIS are depicted in Figure 3.1 together with their meaning according to the ANSI standards:

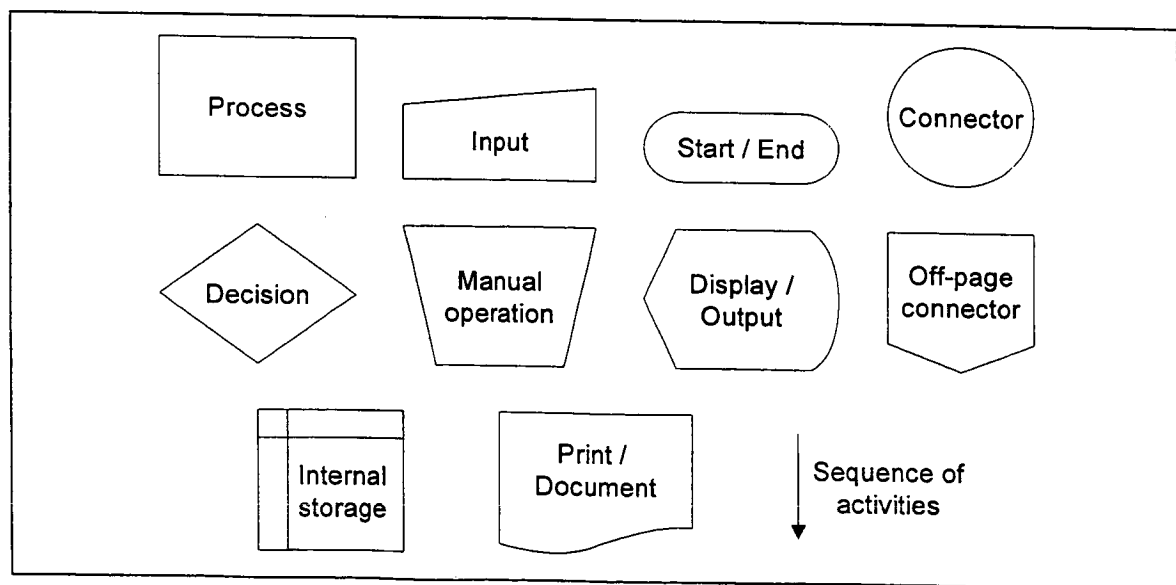


Figure 3.1: Flowchart symbols and their meanings (Whitten *et al.*, 1989).

Another cause for using flowcharts in the development of PSMIS is because, given the appropriate diagramming techniques, it is much easier to describe complex activities and procedures in diagrams than in text (Martin, 1987). A picture can be much better than a thousand words because it is concise, precise and clear. Furthermore, systems flowcharts are the basis for communication between end-user, systems analysts, computer operations personnel and computer programmers (Whitten *et al.*, 1989).

3.3 Overview of the CHTFPM Program Utilization

This section presents an outline and a general idea of the underlying theory of the CHTFPM, which consists of identifying the dendritics of a system—the building blocks of hazards. Founded on this rationale, the first step of the PSMIS, or CHTFPM MIS, is to construct the list of dendritics based on the reports of the PHA, FMEA and barrier analysis. Second, sampling has to be carried out to determine the number of samples needed for statistical significance and to establish the control limits. From these preliminary samples, a Pareto diagram can be constructed according to the cumulative frequencies of the observed dendritics.

In order to conduct the initial observations, the computer program provides the user with sampling sheets in the form of reports to document the occurrence of dendritics. After deciding to set up the control limits, the type of control chart must be selected so that the respective control chart parameters can be calculated. Once the type of control chart has been chosen to represent the safety status of a system, the control limits can be computed and implemented to measure the safety level of the process. Before plotting

points on the control chart, a safety sampling scheme must be created in order to begin collecting data. Such data will be mapped on the control chart after the sampling plan has been developed.

From the acquired information using the designed sampling scheme, a Pareto diagram can be obtained to depict the dendritics that occur more often. When plotting the points on the control chart, it can be seen if the system is in-control or not. If the system is in-control, sampling can continue without any problems. However, if the control chart shows that the system is out-of-control, an investigation must take place to encounter the causes that originated such alarm; the sampling sheets can aid in finding the source(s) that gave birth to an out-of-control point.

If it was determined that the point outside the control limits is an irrelevant or minor reason, then that point is called an outlier, which simply means that system is safe or stable and as a result that point can be ignored. Hence, no changes or corrections are required, and the current control limits can be employed for upcoming monitoring and control.

If it was concluded that the out-of-control point is an assignable cause (special cause not part of a process), it denotes that the system is operating under the presence of hazards; thus, an accident or system failure can occur. In this situation, it is necessary to take immediate action and fix the problem that provoked the hazardous condition(s). As soon as corrections have been made to the process or system, new control limits have to be created, and new dendritics have to be identified if necessary. Figure 3.2 summarizes in a flowchart the entire description of this section.

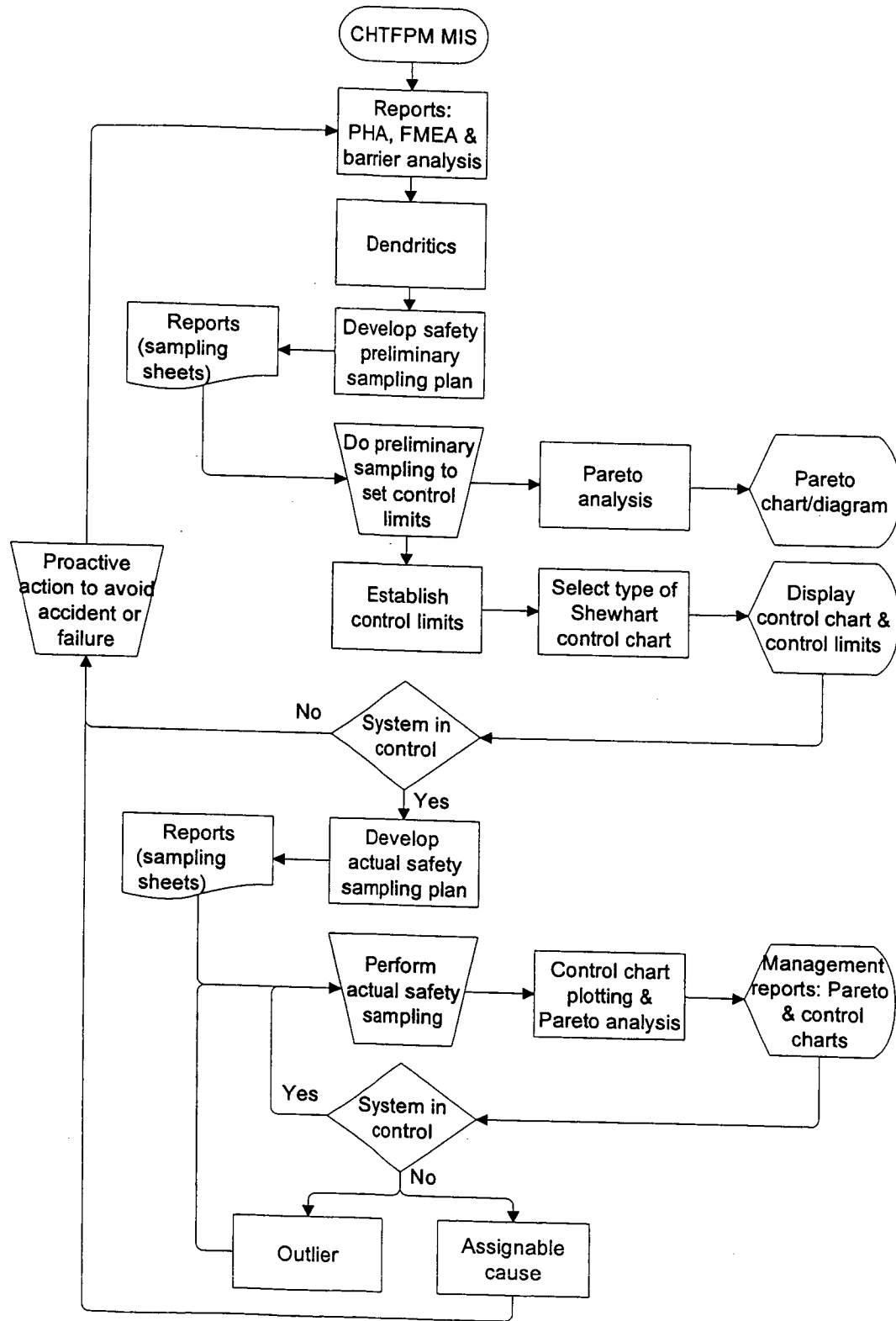


Figure 3.2: Flowchart of the entire CHTFPM MIS general process

3.4 General Overview of the PSMIS

The PSMIS consists of four main tasks, which are the basic and general functions of the program. In order to facilitate the usage of PSMIS and the handling of information, the system was broken down into four major events, which are given below:

- Create a new project.
- Edit a project.
- Delete a project.
- Exit program

Each of these events is described in greater detail in the following sections of this chapter, but the trivial tasks, such as “Delete a project” and “Exit program”, are briefly stated in this section. In addition, the beginning portion of the “Create a new project” action is also explained in this section since it is deemed necessary to understand the total functioning of the PSMIS. Moreover, the user has to deal with this segment of the program, for it is fundamental when realizing a safety project because the end-user has to specify the project number or the project name among other fields, as it is explained later in this section.

The scheme that represents the primary actions in the PSMIS is shown in Figure 3.3. These principal actions are the main events of the CHTFPM computer program; thus, they conform the main menu of the PSMIS as illustrated in Figure 3.4, which represents the flowchart of Figure 3.3.

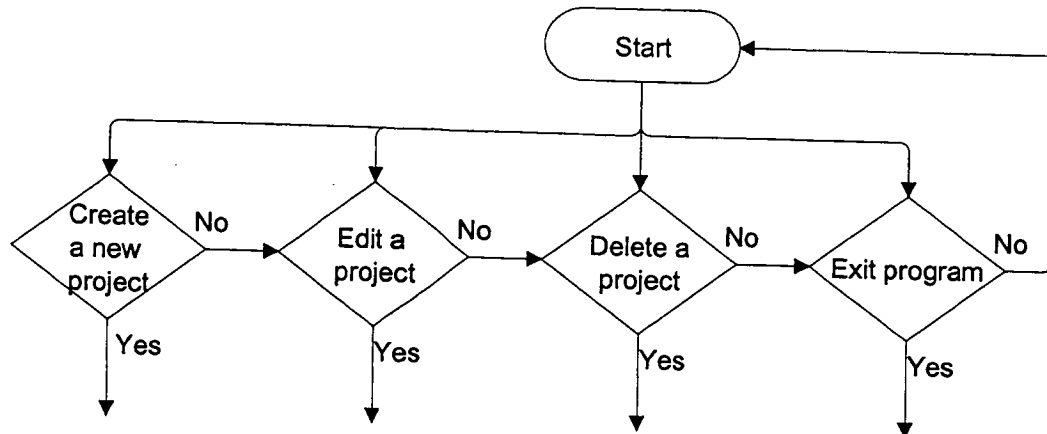


Figure 3.3: Schematic of the core events of the PSMIS.

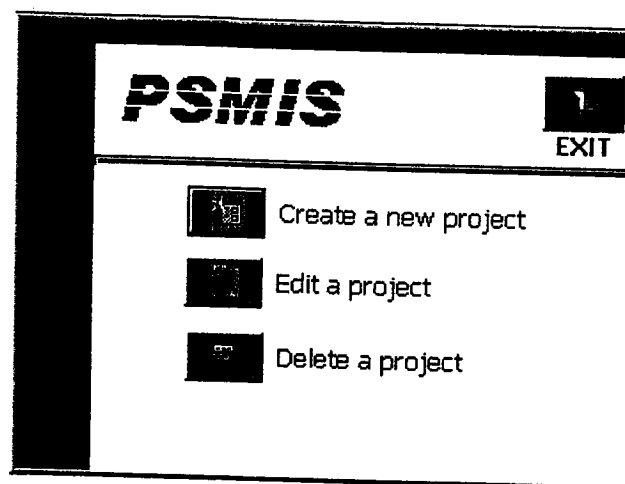


Figure 3.4: Main menu of the PSMIS.

The “Delete a project” characteristic of the PSMIS (CHTFPM MIS) simply executes the action of erasing permanently from the databases all the data related to a particular project. This aspect is portrayed in Figure 3.5. So, when the analyst clicks on the “Delete a project” button, the program asks the user to confirm the deletion action for the selected project, but the person has also the choice to retract from the deletion

process, as seen in Figure 3.6.

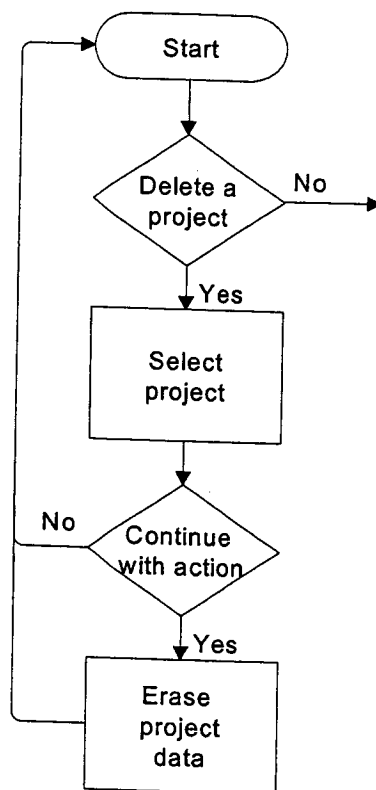


Figure 3.5: "Delete a project" event of the PSMIS.

The screenshot shows a 'Delete Confirmation' dialog box. It contains the following fields:

- Project Number:** 25
- Date:** 27-Feb-03
- Project Name:** Calibration process
- Description:** Valves calibration
- Analyst:** William

Below the fields, a warning message states: "This project is about to be deleted permanently!". To the left of the message is a warning icon (a triangle with an exclamation mark). At the bottom, there are two buttons: "DELETE" and "Abort deletion".

Figure 3.6: Delete window of the PSMIS.

Similar to the previously depicted element, the other simple factor of the principal events is the “Exit program” selection, which is the option that allows the analyst to exit from the program. This feature is very straight forward and self-explanatory; Figure 3.7 illustrates the manner in which the “Exit program” event is carried out.

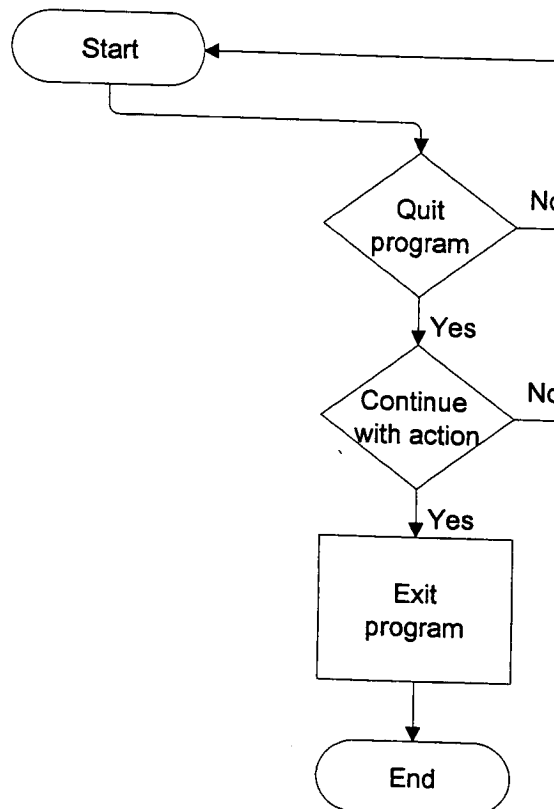


Figure 3.7: “Exit program” event of the PSMIS.

The beginning portion of the “Create a project” attribute is essential when conducting a safety study. The program asks the user to fill out the required fields which are the “Project ID,” “Project Name,” “Description” and “Analyst Name” fields. If these domains are empty the program will not allow the user to continue with the project, as seen in Figures 3.8 and 3.10.

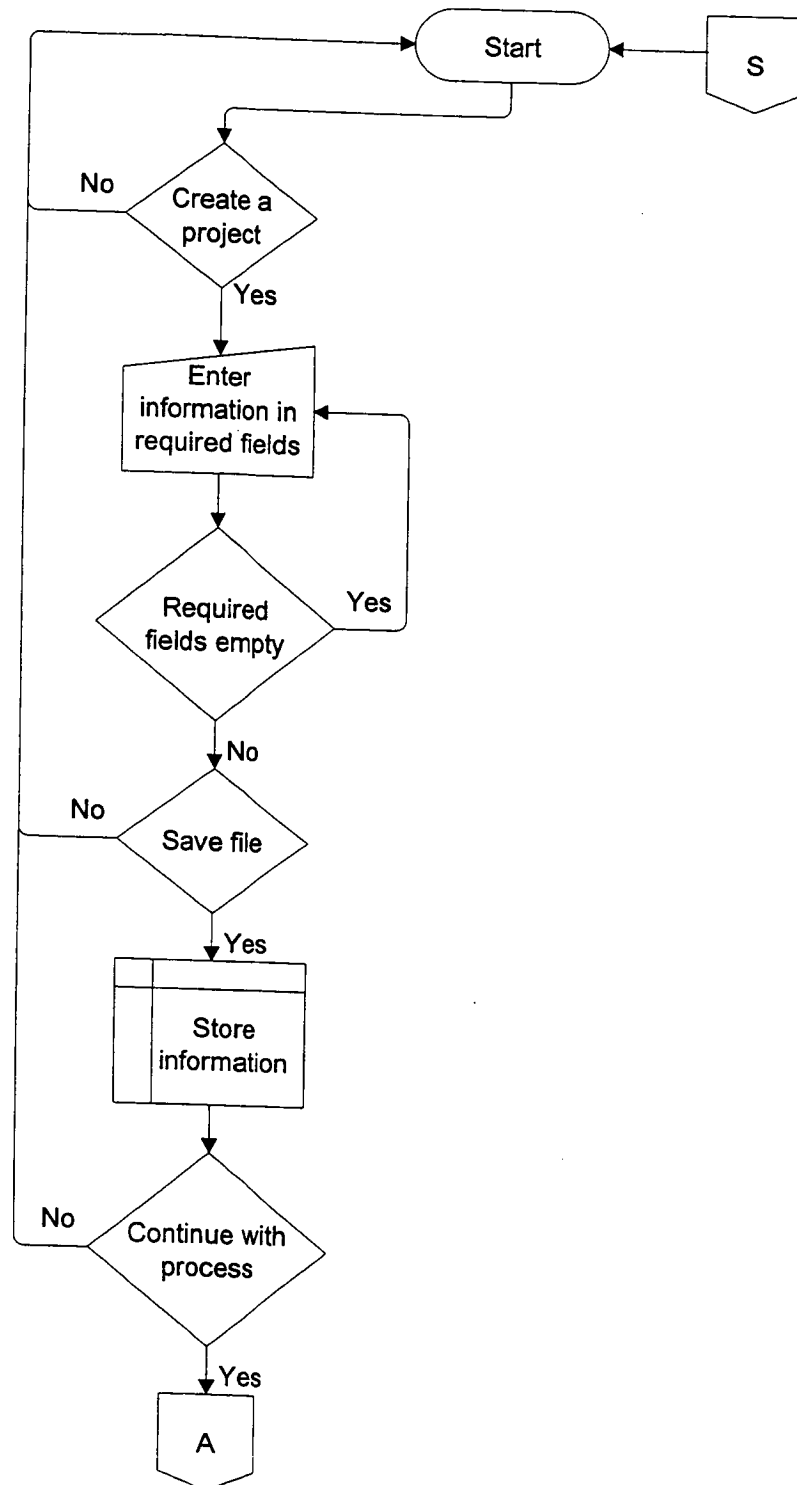
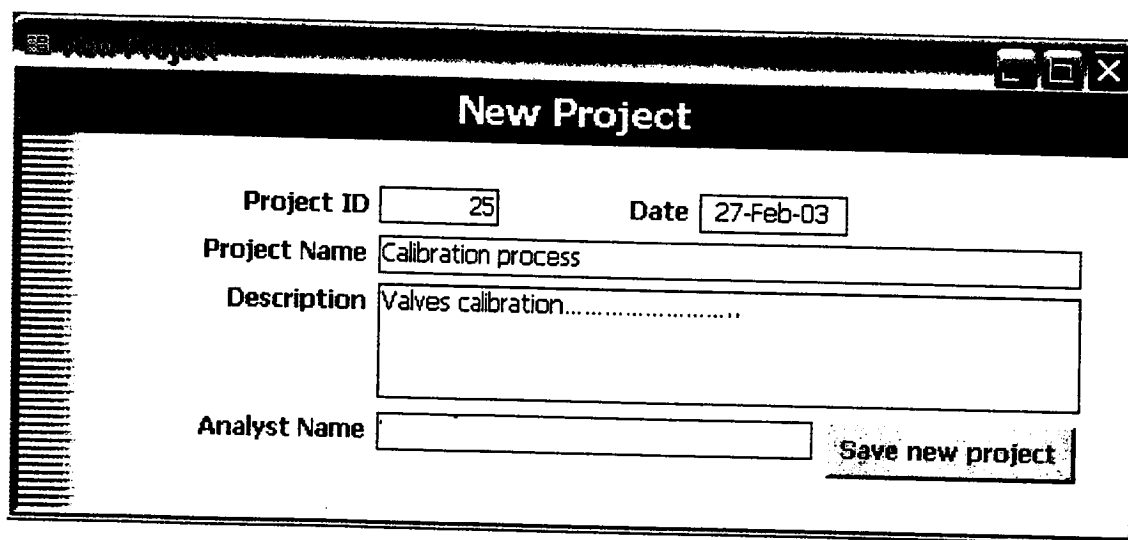


Figure 3.8: Beginning portion of the "Create a new project" event of the PSMIS.

Additionally, Figure 3.9 depicts the information fields of a project that must be filled when commencing a new project. The “Project ID” feature is the most important entry, for it is the identification (ID) number/name by which all projects are classified and recognized. In other words, the project ID is the quality that distinguishes one project from another and helps preserve the integrity of the system; therefore, the program will forbid the repetition of a project ID. Figure 3.10 is an example of a message box that the PSMIS displays when a required field is empty—in this case the “Analyst Name” field supposedly was not filled out.



The screenshot shows a window titled "New Project" with a standard Windows-style title bar. Inside the window, there are several input fields and a button. The "Project ID" field contains the number "25". The "Date" field contains "27-Feb-03". The "Project Name" field contains "Calibration process". The "Description" field contains "Valves calibration.....". The "Analyst Name" field is empty. A "Save new project" button is located at the bottom right of the form area.

Figure 3.9: New project information screen.

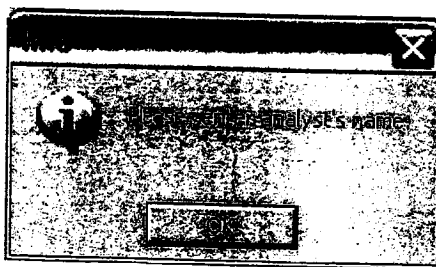


Figure 3.10: Message box indicating that a required field is empty.

3.5 Dendritic Construction

The fundamental issue in the implementation of the CHTFPM is the identification of the core conditions leading to hazards in any given system; these core conditions can be termed as the dendritics of a particular class of hazards. If dendritics are present in a system, they may lead to a hazardous condition, which ultimately can result in an accident or system malfunction. To develop the dendritic list for a system, a thorough study of the system must be performed using established system safety analysis tools, such as the PHA, FMEA and barrier analysis (see Section 2.3). The CHTFPM strongly relies on these techniques for dendritic construction (Quintana *et al.*, 2001), as it is illustrated in Table 3.1.

Table 3.1: Techniques for dendritic construction (Quintana *et al.*, 2001).

Technique	Dendritic Construction
PHA	Identifies safety critical areas, evaluates hazards, and identifies the safety design criteria to be used.
FMEA	Systematic approach that identifies potential failure modes in a system. Focuses on conditions that can lead to hazardous situations.
Barrier Analysis	Effectively identifies root cause of an unwanted event or problem. Extremely useful in programmatic or system analyses involving human interaction with the overall system.

The record of dendritics is elaborated by analyzing and reviewing with detail each entry of the PHA, FMEA and barrier analysis. Afterwards, a preliminary dendritic list is formed by choosing the items that will lead to possible occurrences which could result in system failure or employee injury. Finally, the initial dendritic record is double-checked

for any repeating or similar elements and to enhance the wording of the items, ensuing in the concluding version of the dendritic list. Nevertheless, the final list of dendritics can be modified if more defects or hazardous conditions are found since undetected or new hazards may arise. As indicated by Lee *et al.* (1998), sometimes as the procedure advances in an operation, more detailed assessment of hazards has to be performed. All this process has to be done by the analyst either by hand or by typewriting the information. This procedure is long and some times tedious; however, it is necessary in order to identify the dendritics of the system or process.

On the other hand, the PSMIS can accomplish the dendritic construction automatically and faster. The mode to achieve this course of action is revealed in Figure 3.11, which is the continuation of the “Create a new project” event flowchart in Figure 3.8. Further, to elaborate the inventory of dendritics, the user has two alternatives.

First, the analyst can choose to perform one or all of the analyses forms: PHA, FMEA or barrier analysis. If he or she did so, then the program will enable the user to create the dendritic list from the information entered in the forms with the push of a button called “Import Dendritics.”

The second option the end-user has is to create directly the dendritic list without having to fill out any of the previously mentioned safety sheets; that is, he or she will specify the dendritics or core conditions that could lead to a hazard according to his/her own judgment. In addition, the CHTFPM MIS has the capability of allowing the analyst to modify the list by adding, deleting or editing (rephrasing) dendritics. Moreover, if the end-user altered the dendritic list and does not like the result of it, the person can reset or

go back to the original dendritic list; as seen in Figure 3.12.

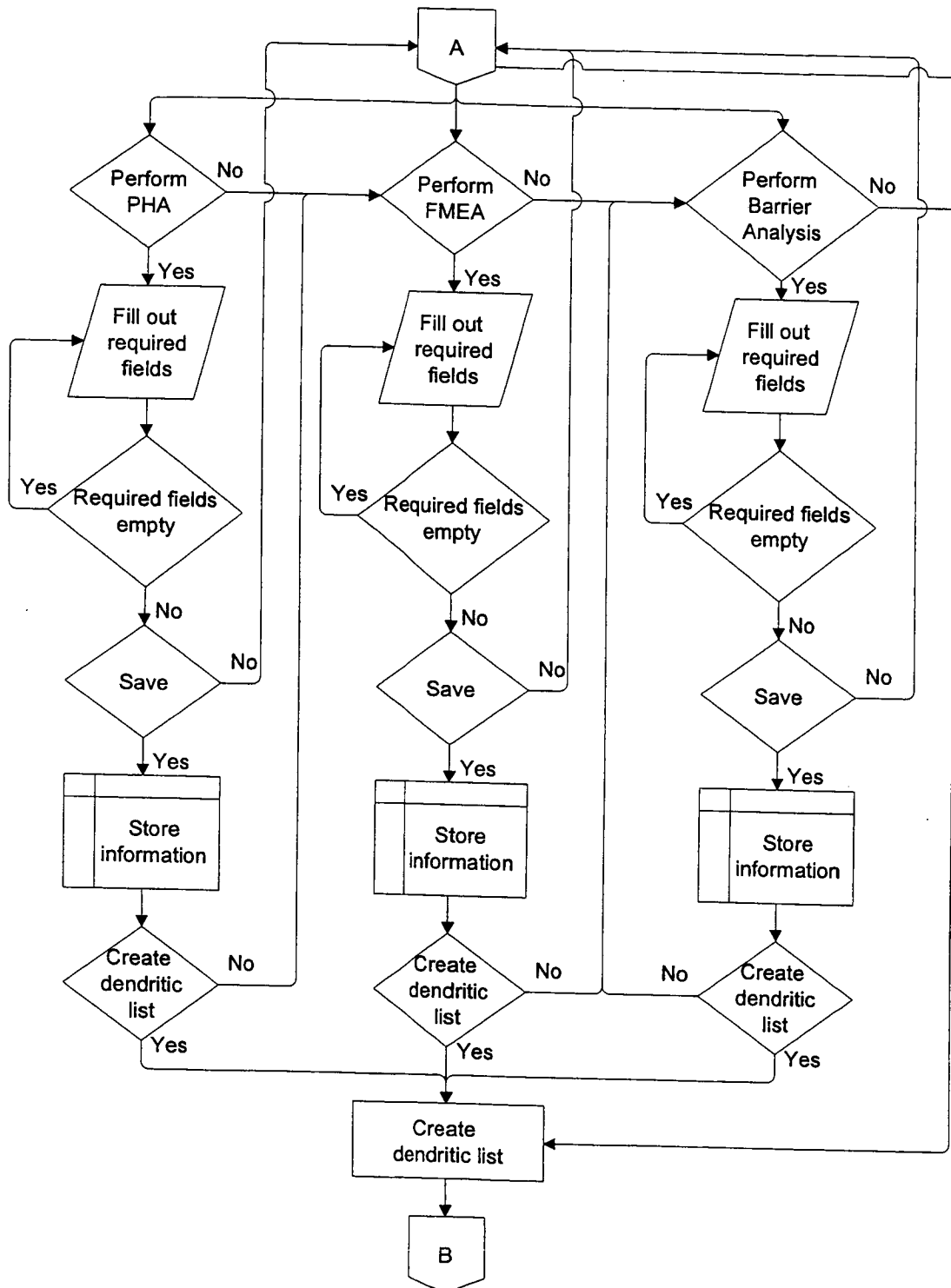


Figure 3.11: Dendritic construction process in the PSMIS.

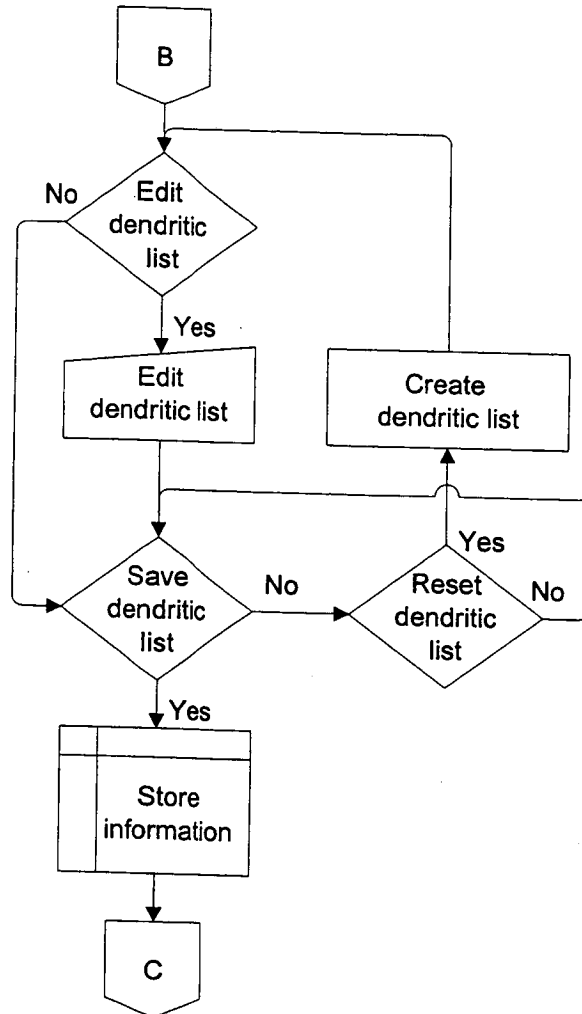


Figure 3.12: Edit feature for the dendritic list.

Another vital step in constructing dendritics is the aspect of adding weights to them because weighting the dendritics can help identify the more serious problems from the less serious. The recommended demerit scheme by Montgomery (1996) was used in this study to partition dendritics into four classifications (see Section 2.4) which, in fact, is the same plan the CHTFPM MIS uses as default. Once the nonconformities or dendritics are separated into categories, each class is weighted or assigned demerits. A weight is assign to a dendritic corresponding to its classification. For example, the

highest weight will be designated to the dendritics that are judged to be in the “very serious” class; on the contrary, the lowest weight will be appointed to the dendritics or defects in the category of “not serious”. The following demerits or weights for each class of dendritics are widely used in practice (Montgomery, 1996) and were the ones employed in this research:

- Class “A” defects (dendritics) – 100
- Class “B” defects (dendritics) – 50
- Class “C” defects (dendritics) – 10
- Class “D” defects (dendritics) – 1

According to these weights, the number of demerits in every observation can be defined as (Montgomery, 1996):

$$d_h = 100c_{hA} + 50c_{hB} + 10c_{hC} + c_{hD} \quad (3.1)$$

where

c_{hA} is the number of Class A defects (dendritics) occurred in observation h .

c_{hB} is the number of Class B defects (dendritics) occurred in observation h .

c_{hC} is the number of Class C defects (dendritics) occurred in observation h .

c_{hD} is the number of Class D defects (dendritics) occurred in observation h .

Since the previously recommended weights are broadly utilized in studies, the PSMIS uses the same demerits as the default values for the dendritics. Nevertheless, the software application enables the user to assign other weights—different from the default values—to the dendritics as the analyst deems appropriate. As a result, the weight values

of Equation 3.1 will change, correspondingly, to those chosen by the user. From the computer program standpoint, the procedure of assigning weights to each dendritic, after the dendritic list has been completed, is carried out in the fashion and sequence that shows Figure 3.13.

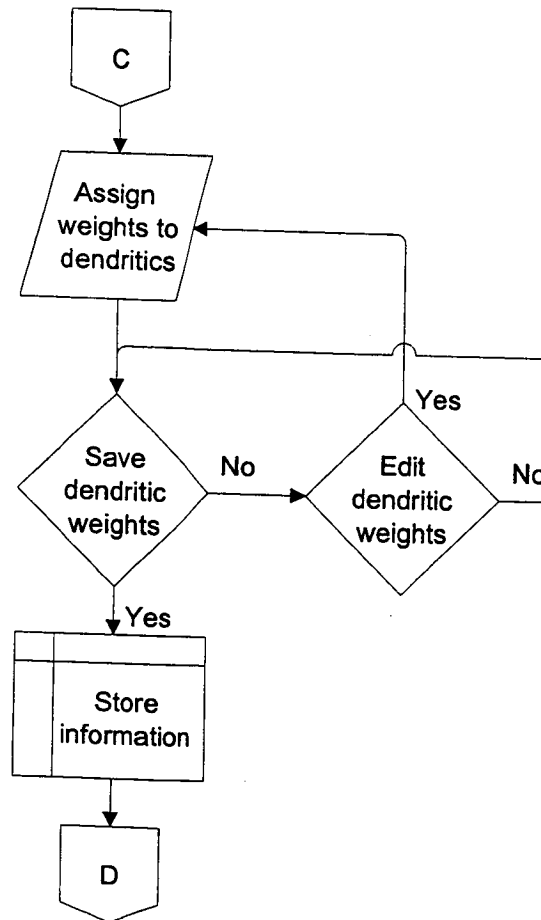


Figure 3.13: Flowchart for assigning weights to dendritics.

3.6 Safety Sampling

The CHTFPM is a concept of providing safety condition information in a statistical and economical manner by using the principles of safety work sampling. The

Industrial Engineering Terminology Standard Z94.12 defines work sampling as “an application of random sampling techniques to the study of work activities so that the proportions of time devoted to different elements of work can be estimated with a given degree of statistical validity” (Shell, 1986). A safety sampling study consists of a large number of observations taken at random intervals or times. In taking the observations, the state or condition of the object of study is noted and conclusions can be drawn.

Sampling is the process of drawing inferences concerning the characteristics of a mass of items by examining closely the characteristics of a somewhat smaller number of items drawn from the entire mass, also termed as the population or universe (Williams, 1978). In general, there are three common methods of drawing samples (Kolarik, 1999):

1. Random Sampling: One or more sampling units selected from a population according to some specified procedure. The sample is considered random if the laws of chance govern its selection. That is, each sampling unit from the population has an equal chance of being selected. For example, picking an apple from a basket filled with apples would be a random sample. Each apple has the same probability of being picked without any apparent preference.
2. Systematic Sampling: A method in which a regularly ordered interval is maintained between items chosen. An example would be selecting every tenth part that exits an assembly line.
3. Stratified Sampling: A method which classifies the population units into a certain number of groups, called strata, and then selecting samples independently from each group or stratum. The division of the population into strata is usually done in

such a way to reduce the variability of the sampled statistics. For example, the use of regular intervals between samples can be applied, with judgmental modifications, when it is thought that process disruptions are more/less likely to occur.

Random sampling is the ideal method for sampling because a sample taken at random from a large group tends to have the same pattern or distribution as the large group or universe. This means that in taking random observations, the state or condition of a process under study is noted with a high degree of confidence if the sample size is large enough. As a result, from the proportion of investigations, conclusions can be drawn concerning the total work activity under consideration (Barnes, 1957).

In addition, random sampling is a cost-effective tool in analyzing a system since it does not require any additional allocation of resources (Quintana *et al.*, 2001). Random sampling is also cheaper and faster than a complete observation, also called a census, because it is usually only a fraction of the group size (Williams, 1978). Consequently, the random sampling method is by far the most commonly used sampling method in industry today (Vining, 1998). Therefore, random sampling is the method that the PSMIS will use to develop a sampling plan. The style in which random sampling will be performed is by defining the number of subgroups and the number of samples per subgroup, which will be elucidated shortly.

3.6.1 Groups, Subgroups and Observations per Subgroup

Subgrouping is important because it permits to obtain enhanced statistical performance in control charts; such enhancement refers to reducing the chance of failing

to detect a dendritic or assignable cause in a given system or process, according to Kolarik (1999). Subgrouping is also valuable because it provides a statistical test to determine whether the variation from subgroup to subgroup is consistent with the process mean and the average variation within the subgroups (Grant and Leavenworth, 1996). In addition, the most obvious rational basis for subgrouping is order of production or time order (Montgomery, 1996), which is an organized list of random times that are arranged in sequence or succession. Therefore, according to the rationale presented before, time order is the logical basis that the PSMIS employs for data collection.

The sample size should be chosen in a way that appears likely to give the maximum chance for the observations in each subgroup to be alike (Montgomery, 1996). In other words, the choice of subgroup size should be influenced, in part, by the desirability of permitting a minimum chance for variation within a subgroup. In most cases, more useful information will be obtained from, say, five subgroups of 5 inspections than from one subgroup of 25 observations. In large subgroups, such as one of 25 observations, there is likely to be a much greater opportunity for a process change within a subgroup (Quintana *et al.*, 2001).

In many occasions, subgroups of 4 inspections are adequate and sufficient for deriving reliable conclusions. Subgroup sizes of 4 (± 1 observations) are extremely helpful to determine whether or not a group of measurements is statistically homogeneous, for the possibility of a large variation within a subgroup is considerably less. Subgroups of size 4 also allow a maximum chance for the subgroups to differ one from the other (Montgomery, 1996). Since subgroups of size 4 are widely used in

practice, the PSMIS recommends this criterion as the subgroup range. Nevertheless, the analyst can choose any other subgroup size.

For example, if a safety study is to be conducted in an assembly line of a manufacturing plant for 5 days (assuming each day has one shift of 8 hours), then the study could be broken down into 5 groups (days) of 8 subgroups (hours) each. The number of observations per subgroup would be selected by the analyst, say 4. Therefore, each observation would be represented by a random time in which an inspection would take place to look for any dendritics present in the system at that moment. This means that each subgroup would be conformed of 4 arbitrary times (observations).

It is fundamental to mention that the subgroup values are the points plotted in a control chart in relation to the characteristic of the particular Shewhart control chart being used. For instance, the p chart plots the fraction of dendritics and the \bar{u} chart plots the average of dendritics in each subgroup, but the c chart plots the number of defects per subgroup (Section 3.7 provides a thorough description of this aspect). Developing plots of subgroup means may appear counter intuitive from a physical perspective; however, it is essential because it makes a great deal of sense from a statistical point of view since precision is gained (Kolarik, 1999). In addition, the center line is the process mean, and it is also computed based on the distinguished quality of the respective attribute (Shewhart) control chart.

3.6.2 Preliminary Sampling Plan

Initial or introductory samples are indispensable to achieve statistical confidence

in a safety study. Thereby, it is first required to develop a preliminary sampling plan in order to conduct initial observations. This introductory sampling scheme involves random times, at which the inspections will be carried out. The random times can be generated by the CHTFPM MIS or by the analyst with the aid of a programmable, random beeper or any other device, as shown in Figure 3.14.

In the event that the first choice is made, the end-user can modify the random times if these are not right. This capability is helpful in occasions when an arbitrary time resides in a moment that is inappropriate. For instance, if observations will be conducted in a production line of an industrial plant, it may be possible that a sampling time will be listed at a period when the operators are scheduled to take a break; therefore, that random time will fall at an improper instant. If this happens, it is necessary to edit or change that specific time to a suitable moment (see Figure 3.14); nevertheless, the system analyst can also disregard that particular time if he or she does not want to correct it.

On the other hand, if the second approach is followed, the user will have to record the random times whenever the beeper makes a sound and input those times later into a table that was created by the computer program. That is, the worksheet where the random times are placed (table for random times) stays vacant—since no times are generated—so the analyst can enter the beeper times at a later instant. Previous to input the random beeper times into the computer, the CHTFPM program combines the dendritic list and the table for random times in order to build a form or sheet for data collection. This form can be printed to register the data from the initial observations if the inspection site is away from the computer; then such information can be input afterward into the software along

with the random beeper times (refer to Figure 3.15). In addition, if the user does not like the set of random times, for any reason, the individual can create a new list of arbitrary times, as illustrated in Figure 3.14.

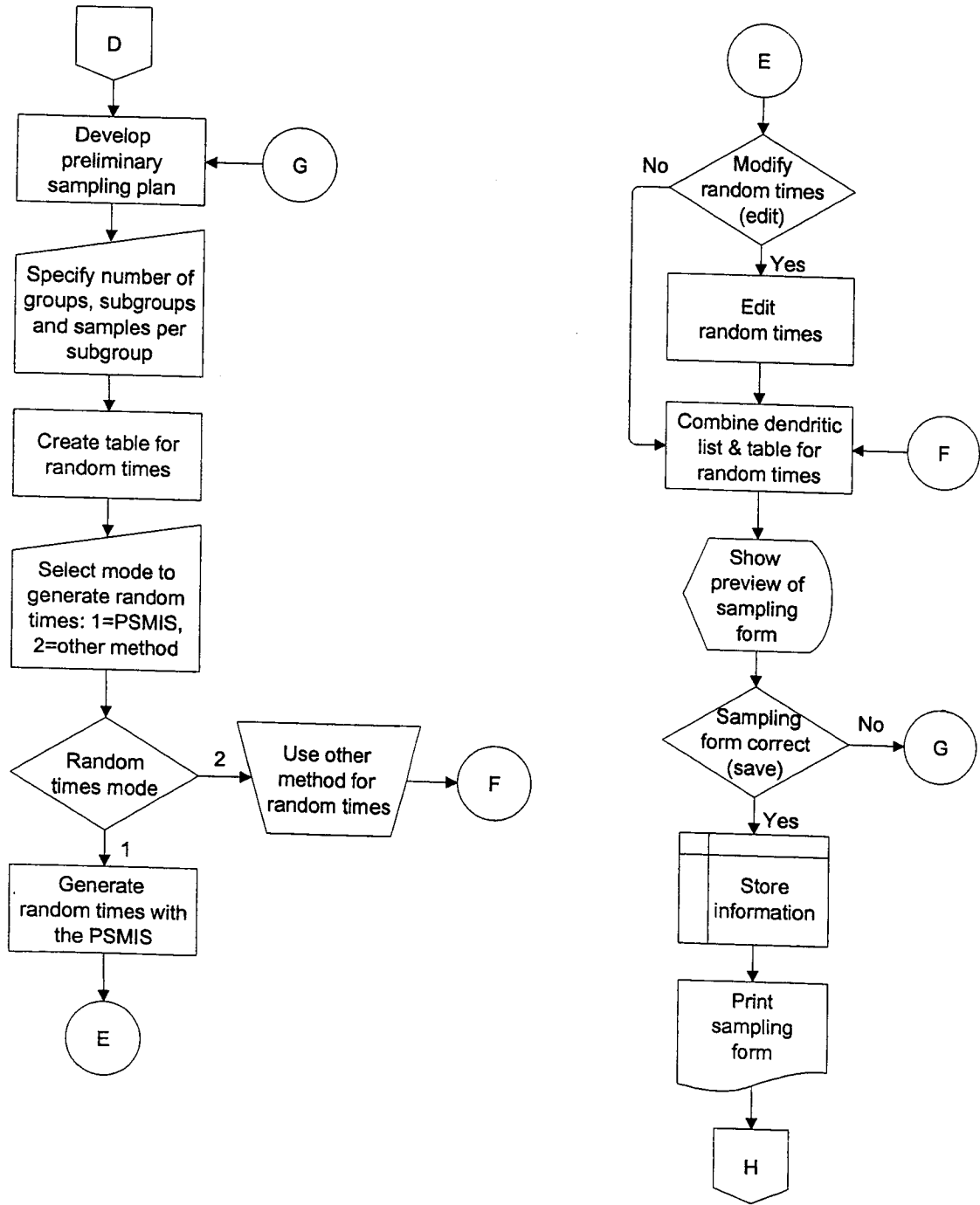


Figure 3.14: Flowchart of preliminary sampling plan.

3.6.2.1 Sample Size for Statistical Significance

A calculation of the number of samples necessary to attain statistical significance is a substantial element of the validity of the model. To calculate the number of observations needed, n' (*n prime*), to achieve statistical dependability, it is a requisite to carry out initial samples in order to collect data from dendritic occurrences. Nonetheless, before calculating n' , it is obligatory to know the percent of dendritics present (\hat{p}). Furthermore, prior to determining \hat{p} , the system assessor must specify to the software program the length of the confidence interval (CI), L' , and confidence level (CL), thus the error percent ($\alpha' = 100[1 - CL] \%$), which is the accuracy desired for statistical impact.

The CL and α are required to decide what level of certainty is desired in the final results; further, the number of samples depends on these two values. The confidence level is the probability that the true parameter may occur within the specified percent range under the standard normal distribution curve. Additionally, the L' , and CL values can be changed by the analyst at any moment throughout the realization of a project, but the respective, previous results will be affected, accordingly. The following equations depict the necessary calculations for determination of the minimal sample size (Devore, 1995):

$$\hat{p} = \frac{\text{Number of dendritics observed in the preliminary sampling}}{(\text{Total possible dendritics per observation}) * (\text{Number of observations})} \quad (3.2)$$

$$n' = \frac{4(z'_{\alpha/2})^2 \hat{p}(1 - \hat{p})}{(L')^2} \quad (3.3)$$

where

L' is the length of the confidence interval (CI) for \hat{p} .

$Z'_{\alpha/2}$ is the value of the measurement axis for which $\alpha'/2$ of the area under the standard normal curve lies (Devore, 1995).

The previous equations are integrated into the CHTFPM code as well as the equations for the control limits (view Section 3.7). Therefore, such reckonings will be performed automatically by the PSMIS. Hence, the analyst can know at what point statistical significance has been achieved. Figure 3.15 describes the organization and sequence of this process.

3.6.2.2 Establish Control Limits

In order to establish the safety control limits, a preliminary set of observations must be performed. This is also done to find out the minimum number of observations or inspections required to have statistical reliability (n'), based on the desired L' and CL specified by the analyst. The resulting number of n' is then compared with the acquired sample size of the preliminary investigation, n , to verify that enough inspections have been performed. If the required amount of observations has not been reached, the process of acquiring data should continue until the essential number of samples has been taken.

However, the system evaluator, at any point, can choose to establish the control limits even if the actual number of samples (n) does not match the number of inspections needed (n'). In other words, the user can view the actual error percentage, α , that corresponds to the actual number of samples, n , that have been taken. If the individual deems that the real error proportion (α) is acceptable, then he/she can decide to set up the

control boundaries even though the required quantity of observations (n') has not been attained, as shown in Figure 3.15.

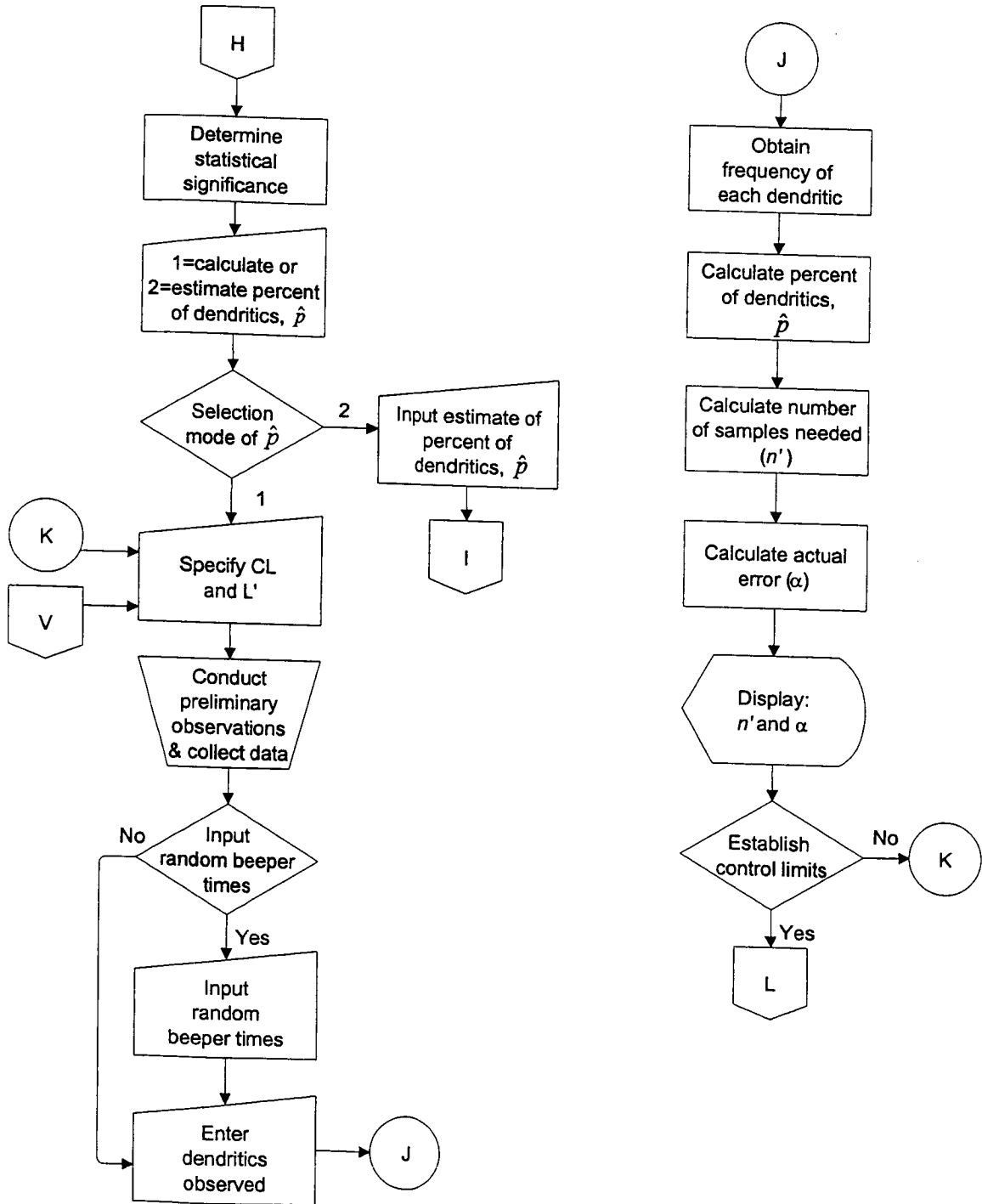


Figure 3.15: Flowchart to calculate number of samples needed for statistical significance.

In addition, the system analyst can also choose to specify the proportion/percent of dendritics, \hat{p} , to find the number of samples needed (n'). This means that the user can input an estimate value of \hat{p} before conducting the preliminary observations, but the subsequent recalculations of \hat{p} , if necessary or requested, will be obtained based on the data gathered from the preliminary data set. If the analyst decides to take this path to calculate n' , the software will tell the system evaluator the number of samples that must be taken according to the proportion or percent of dendritics, \hat{p} , that he or she predicted, as observed in Figure 3.16. Then the individual can perform the number of samples needed for statistical importance.

If the person opts to conduct less observations than the ones stated by the computer program (based on the approximation of \hat{p}), the CHTFPM MIS can know the computed percent of dendritics, \hat{p} , in the preliminary data set. With the \hat{p} value, the PSMIS can also calculate the actual error percentage (α) that corresponds to the actual number of observations conducted (n). Thereafter, it is up to the analyst to determine whether or not to set up the control limits even though the user did not carry out the required amount of samples (n'); Figure 3.16 portrays this PSMIS procedure when \hat{p} is estimated. Once all this is accomplished, the control limits can be calculated by the software application (see Figure 3.17) and the analyst can proceed with actual sampling in the manner described in Section 3.6.3.

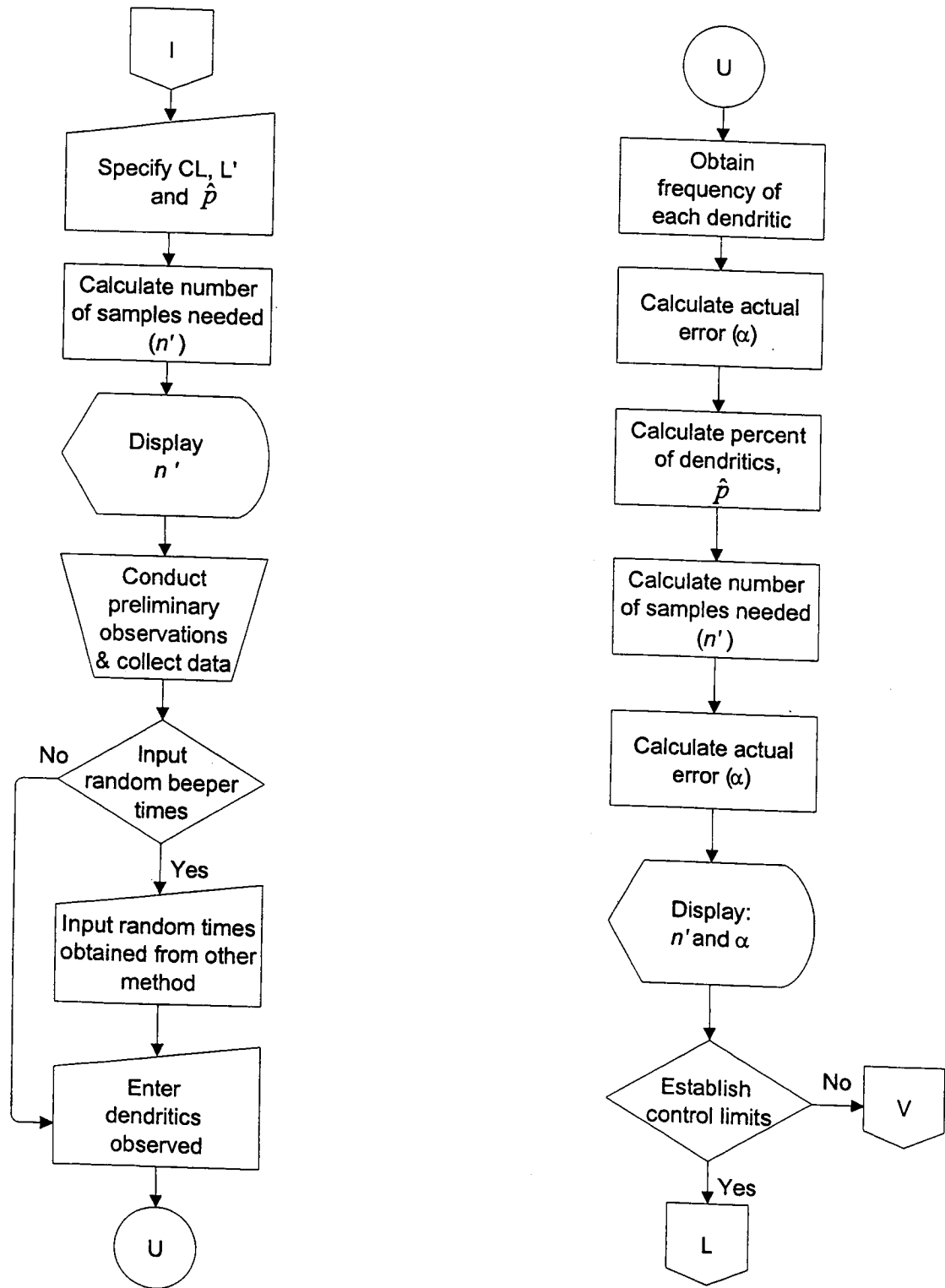


Figure 3.16: Process that the PSMIS follows when the user estimates \hat{p} .

3.6.2.3 PSMIS Process to Establish Control Limits

The equations for calculating the control limits of all control charts are integrated in the CHTFPM code as well and are depicted in Section 3.7. Therefore, such reckonings will be performed automatically by the software system. The CHTFPM MIS executes the respective computations—center line, LCL, and ULC, *etc.*—depending on the type of chart selected. Once the user chooses to establish the control limits, the person needs to select the type of Shewhart chart that will represent the collected data.

After the preliminary sampling has been terminated, the PSMIS offers the user four options. The analyst can view the control limits as well as the plotted points for any of the four attribute control charts—*c*, *p*, *u* or weighted chart—except the EWMA chart (review Section 3.7.7 for a clarification on this subject). By having the accessibility of viewing the plotted points of a control chart of the preliminary data, the analyst can observe if there are any out-of-control points (Section 3.8 elucidates how to deal with points out of control).

A control chart is constructed graphically by plotting a point or characteristic that has been measured or computed from a sample (*e.g.* number of dendritics in subgroup 1) versus the corresponding sample number (*e.g.* subgroup 1). The CHTFPM MIS will plot the chart points according on the attribute chart that is selected. Therefore, even though the control charts values are plotted in subgroups, each Shewhart chart has a different way to calculate the subgroup values (refer to Section 3.7 for a detailed explanation of these characteristics). In addition, Figure 3.17 represents the manner in which the PSMIS establishes or calculates the center line and control limits in order to make them available

for the analyst to see.

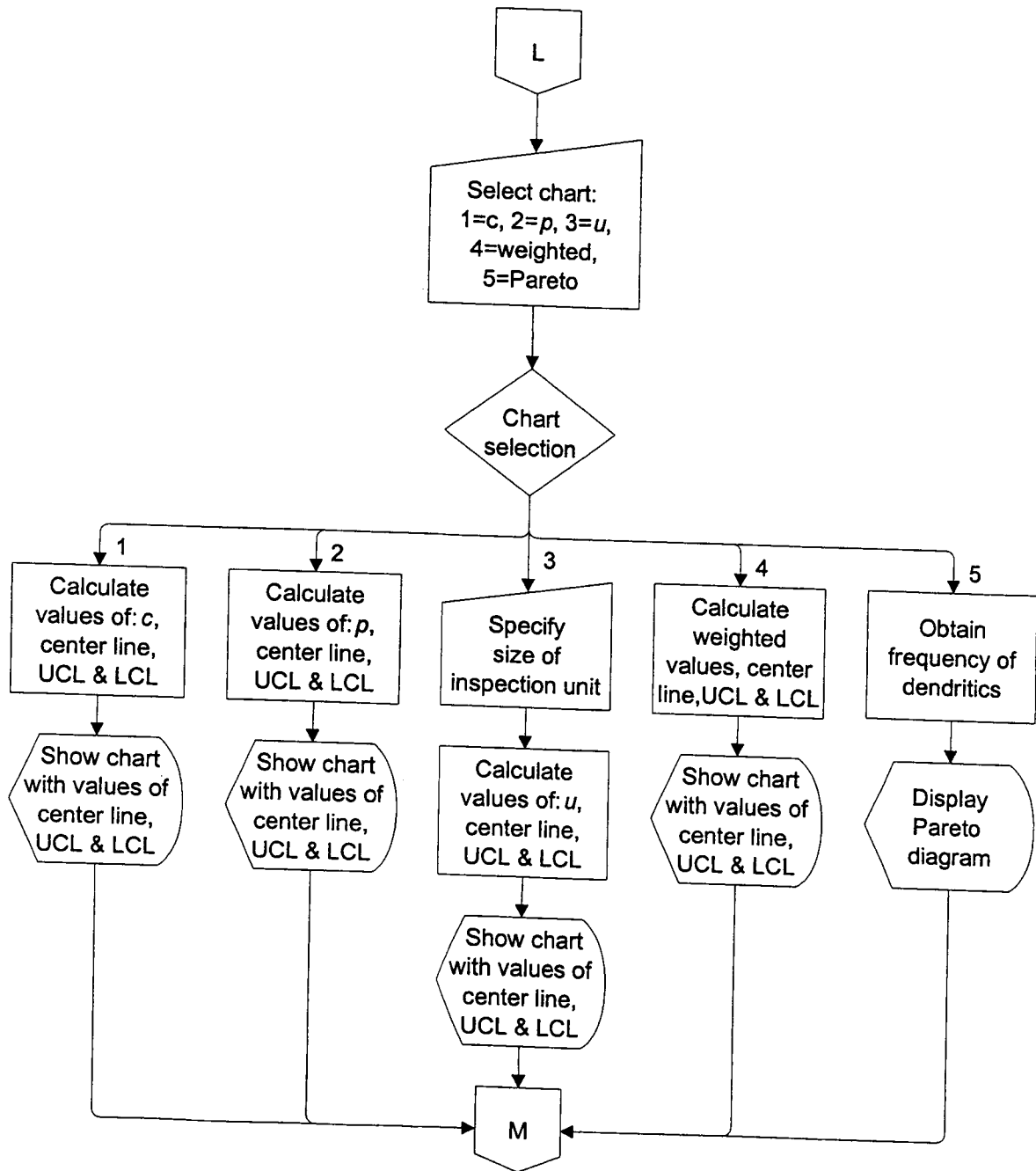


Figure 3.17: Flowchart for the calculation of the control limits.

Additionally, at this stage of the PSMIS, a Pareto diagram is available, as shown in Figure 3.17. This implies that the number of dendritics observed during the

introductory samples will be tallied. The Pareto chart is an excellent tool for classifying process upset causes by ordering the most frequently observed dendritics from highest to lowest (see Section 3.6.4). Thus, the Pareto analysis is a useful tool for prioritizing process improvement effort (Kolarik, 1999).

3.6.3 Actual Sampling Plan

The same procedure used in the preliminary sampling scheme must be exactly followed to design the actual sampling plan. It is necessary that both the preliminary and the actual sampling plans have equal sample size; that is the same number of observations in each subgroup. Otherwise, the user will only be allowed by the PSMIS to view a u chart since this is the single control chart that does not carry the restriction of equal sample size (please read Sections 3.7.3 and 3.8.2 to comprehend this matter). Moreover, the actual samples are carried out after the preliminary observations because the CHTFPM MIS executes both sampling schemes separately. However, they are joined together by the PSMIS once the actual observations have been introduced into the software system. This signifies that the subgroup values and control limits obtained in the preliminary data set are plotted with the actual samples concurrently in the same graph.

The CHTFPM MIS prompts the end-user to indicate the desired number of groups, number of subgroups in each group and samples per subgroup. The CHTFPM code takes these specifications and constructs a table where the arbitrary times will be placed, as shown in Figure 3.18. The sampling plan process is identical to the process of the random times for the preliminary samples. Once the preferred number of subgroups

and inspections per subgroup are specified, the software program offers the analyst two options to create a sampling scheme.

The first choice the analyst has is to generate the random times necessary for each observation by means of the PSMIS (see Figure 3.18). If the user takes this course of action, the computer program will create arbitrary times and will place them in the spreadsheet or table previously fabricated. Additionally, just as the dendritic construction portion of the PSMIS allows the user to change or edit the dendritic list, the computer system also permits the analyst to modify the random times if these are not correct. By this, it is meant that in some occasions an arbitrary time may fall within an invalid range.

Using again as an illustration the example of the assembly line previously stated, it may be possible that a sampling time could be scheduled at a period when the operators are programmed to have lunch. Consequently, only that random time(s) would have to be modified or regenerated to a different, but valid, time instead of generating once more the entire random times of the sampling plan.

The second alternative the user has to produce random times is by using a programmable, random beeper or other method. If the analyst decides to pursue this route, the worksheet for the random times will remain empty so that the user can input the random beeper times manually at a later moment. In addition, the evaluator would conduct an observation whenever the pager alarm goes off; however, the individual must notice and record the time, at which the observation was taken, so he/she can input that time afterward in the CHTFPM MIS.

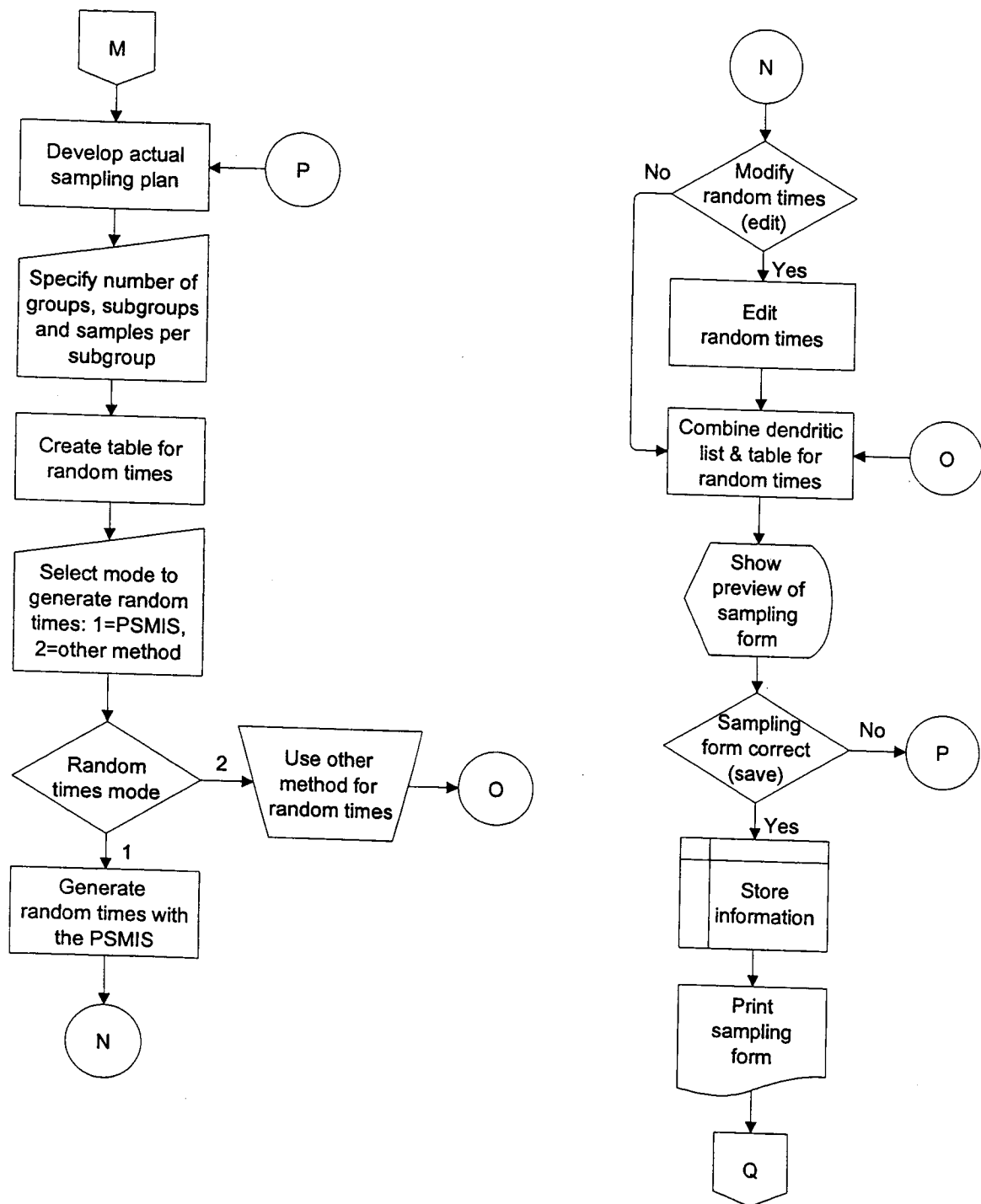


Figure 3.18: Flowchart of actual sampling plan.

After electing any of the two paths for generating arbitrary times, the person conducting the study can preview the sampling form—where dendritics observed are

documented—to verify that everything is correct. If there are mistakes, the end-user can go back and make any corrections as necessary. On the contrary, if the sampling form is correct, it can be printed as a hard copy (view Figure 3.18); thus, observations can be recorded manually and then transferred or input into the computer program as illustrated in Figure 3.19.

3.6.4 Pareto Analysis

The Pareto Analysis is an excellent tool for classifying process upset causes by ordering the most frequently observed dendritics from highest to lowest by means of a Pareto chart or diagram. A Pareto chart is a pictorial representation of a frequency distribution for categorical data (Devore, 1995). A frequency distribution essentially provides a count of only the number of observations of a particular characteristic or category. Each category represents a different type of nonconformity or dendritic. The categories are ordered so that the one with the largest frequency appears on the far left of the diagram, then the category with the second largest frequency, and so on (Devore, 1995). Therefore, a Pareto diagram is constructed using rectangles or bars whose heights are equivalent to the frequencies.

The CHTFPM MIS calculates the cumulative frequency of the dendritics and arranges them from highest to lowest, so the Pareto diagram can be constructed to portray which dendritics occur more frequently compared to others. The rank ordering in the Pareto chart automatically isolates and focuses our attention on the most frequent cause or dendritics (Kolarik, 1999); thus, proactive measures can be taken more specifically for

accident prevention.

Figure 3.19 shows in one of the steps of the process the calculation of the total frequency of each dendritic. This complete Pareto diagram, which includes the incidences of both preliminary and actual sampling plans, is only accessible under the “Management Reports” option (see Section 3.8.1 for a description of this feature). To view the control charts with the entire observation points plotted (preliminary plus actual samples), the same previous submenu has to be selected, which is under the “Edit a project” menu.

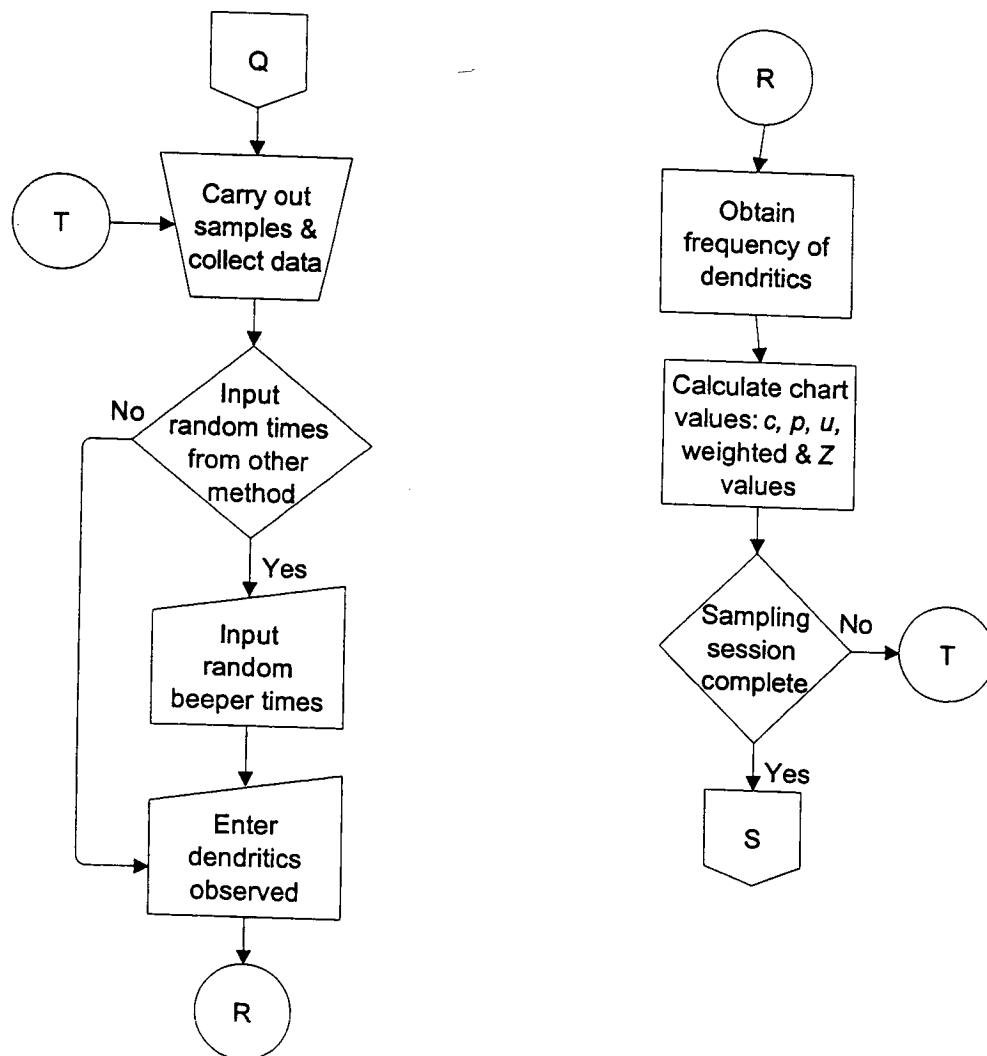


Figure 3.19: Flowchart for calculating total dendritic frequency and entire chart values.

3.7 Safety Control Charts Theory

A system or process operating under the presence of assignable causes is said to be out of control (Montgomery, 1996). An assignable cause is simply something that is not common to happen and that is wrong with the process. Assignable causes in the CHTFPM are the dendritics, or building blocks of hazards. To eliminate an assignable cause, the process must be fixed or repaired (Levinson and Tumbelty, 1997). Statistical process control is used to measure the tendency of assignable causes in a process—to determine if the process is becoming hazardous—and control charts are employed extensively for this task (Wise and Fair, 1998).

A control chart is constructed graphically by plotting a point or characteristic that has been measured or computed from a sample (*e.g.* number of dendritics in subgroup 1) versus the corresponding sample number (*e.g.* subgroup 1). The chart contains a center line that represents the average value of the quality characteristic corresponding to the in-control state (Montgomery, 1996). Two outer horizontal lines, called the upper control limit (UCL) and the lower control limit (LCL), are also shown on the charts. These control limits are chosen so that if the process is in control, nearly all of the sample points will fall between them.

The manner in which these limits are chosen is by selecting the type of control chart, thus a distribution, which would best represent the nature of process or system being analyzed. There are several different types of controls charts (refer to Section 2.5.2.3). Each type of chart has different center lines and control limits. The Shewhart control charts are also called attribute charts; these charts are preferred in industry

because they are universally applicable, and there are three widely used attributes control charts in statistical process control (Wise and Fair, 1998).

3.7.1 Control Chart for Nonconformities

There are many practical situations in which it is preferred to work directly with the number of defects or nonconformities (Levinson and Tumbelty, 1997). The chart that lends itself particularly well for this job in the CHTFPM is called the c chart or control chart for nonconformities. In process control, a nonconformity is a defect in an item or product. An item may have several quality characteristics that are examined simultaneously by the inspector. If the item does not conform to standard on one or more of these characteristics, the item is classified as nonconforming (Montgomery, 1996); hence, nonconformities represent flaws or defects in a product. In the CHTFPM, the nonconformities or defects are the dendritics. If a system is said to be nonconforming, it means that the system is operating under the influence of unacceptable risks or hazards, which are originated from the dendritics.

A criterion of the c chart is that each inspection unit (*e.g.* subgroup) must be of constant sample size. Moreover, this chart assumes that the occurrence of nonconformities, or dendritics, in inspection blocks of equal sample size is modeled by the Poisson distribution (Montgomery, 1996). Essentially, this requires that the number of opportunities or potential locations for dendritics be infinitely large and that the probability of occurrence of a dendritic at any location be small and constant (Grant and Leavenworth, 1996).

A c chart is constructed by plotting the number of dendritics or nonconformities in each subgroup. The parameters of the control chart for the number of nonconformities per inspection segment are as follows (Montgomery, 1996):

$$\text{Center Line} = \bar{c} = \frac{\sum_{i=1}^m c_i}{m} \quad (3.4)$$

$$UCL = \bar{c} + 3\sqrt{\bar{c}} \quad (3.5)$$

$$LCL = \bar{c} - 3\sqrt{\bar{c}} \quad (3.6)$$

where

i is used as a subgroup or sample index.

c_i is the observed number of defects (dendritics) in sample i (m_i).

m is the number of subgroups or samples taken in the preliminary set of data.

\bar{c} is the mean or average of nonconformities (dendritics) per subgroup in the preliminary set of data.

The 3 is present in the control limit formula because the chart is based on three standard deviations (3σ) from the central value. Thus, the UCL and the LCL will have approximately 99.73% of all normal observations within their boundaries, since 3σ means that approximately 99.73% of all observations should be within these limits (Vining, 1998). This 3σ control limit on either side of the center line is commonly used to construct the control charts for work sampling, regardless of its particular use (Montgomery, 1996).

3.7.2 Control Chart for Fraction Nonconforming

The control chart for fraction nonconforming is also known as the p chart. This chart relates to the fraction of nonconforming (defective) items produced by a process; hence, the name of control chart for fraction nonconforming. Unlike the c chart that deals with the number of nonconformities observed per inspection entity, the p chart works with the fraction nonconforming. In other words, the fraction nonconforming is defined as the ratio of the number of nonconforming items in a population to the total number of items in that population (Montgomery, 1996). The statistical principles underlying the control chart for fraction nonconforming are based on the binomial distribution.

Suppose a production process is operating in a stable manner, such that the probability that a unit will not conform to specifications is p , and that successive units produced are independent. Then if there are D_i nonconforming or defective items in sample i , the fraction nonconforming in the i th sample, which is the plotted subgroup value in the p chart, is computed as:

$$p_i = \frac{D_i}{n} = \frac{\text{Number of observed defective items (dendritics) in sample } i (m_i)}{\text{Sample size}} \quad (3.7)$$

where

i is used as a subgroup or sample index.

n is the sample size, which represents the total number of possible defective items (dendritics) in each sample or subgroup.

The center line (\bar{p}) and the control limits for the p chart are given by the following formulas (Montgomery, 1996):

$$\text{Center Line} = \bar{p} = \frac{\sum_{i=1}^m D_i}{mn} = \frac{\sum_{i=1}^m p_i}{m} \quad (3.8)$$

$$UCL = \bar{p} + 3\sqrt{\frac{\bar{p}(1-\bar{p})}{n}} \quad (3.9)$$

$$LCL = \bar{p} - 3\sqrt{\frac{\bar{p}(1-\bar{p})}{n}} \quad (3.10)$$

where

m is the number of subgroups or samples taken in the preliminary sampling.

\bar{p} is the average of all the subgroup proportions of nonconforming items (dendritics) in the preliminary sampling.

3.7.3 Control Chart for Average Nonconformities per Unit

The third kind of control chart is called the control chart for average nonconformities per unit or u chart. This chart is useful in situations where the average number of nonconformities per unit is a more convenient basis for process control (Wise and Fair, 1998); the u chart is designed to deal with this case. A nonconforming item, as it was said earlier, is a unit of product that does not satisfy one or more of the specifications for that product.

Each specific point at which a specification is not satisfied results in a defect or nonconformity (Montgomery, 1996). Consequently, a nonconforming item will contain at least one nonconformity. Since a nonconforming product may have more than one

nonconformity, it is more suitable in some situations to deal with the average number of defects or nonconformities (dendritics) per inspection unit (Montgomery, 1996).

The size of the inspection unit can be $1, 2, 3, \dots, n$ items per sample. In the CHTFPM, the inspection unit size can be $1, 2, 3, \dots, n$ observations per subgroup. This implies that the inspection unit cannot be greater than the subgroup or sample size, n , specified in either sampling plan: preliminary or actual. However, the recommended size of the inspection unit by the PSMIS is 1 (one).

The u chart plots the average number of occurring nonconformities (dendritics) per inspection unit for each subgroup sampled. Similar to the c chart, the u chart is based on the fundamentals of the Poisson distribution (Montgomery, 1996). However, unlike the c and p chart, the u chart does not carry the restriction of equal sample size. In circumstances where sample sizes are not equal, the u chart is the proper chart to use. If u total nonconformities are found in sample i of n inspection units, then the number of nonconformities per inspection unit in a subgroup is:

$$\bar{u}_i = \frac{u_i}{n_i} = \frac{\text{Number of observed defects (dendritics) in sample } i (m_i)}{\text{Number of inspection units in sample } i (m_i)} \quad (3.11)$$

where

i is used as a subgroup or sample index.

$$n_i = \frac{\text{Number of conducted observations in sample } i (m_i)}{\text{Size of inspection unit}} \quad (3.12)$$

The parameters of the control chart for the average number of nonconformities per unit are the following (Montgomery, 1996):

$$\text{Center Line} = \bar{u} = \frac{\sum_{i=1}^m u_i}{\sum_{i=1}^m n_i} \quad (3.13)$$

$$UCL = \bar{u} + 3\sqrt{\frac{\bar{u}}{n_i}} \quad (3.14)$$

$$LCL = \bar{u} - 3\sqrt{\frac{\bar{u}}{n_i}} \quad (3.15)$$

3.7.4 Weighted Control Chart

Although the three previously described charts are the most commonly used Shewhart control charts in practice, there is still one more attribute chart that belongs to this group: the weighted chart. The aspect of adding weights to the dendritics or nonconformities, as it was talked about before, can help identify the more severe problems from the less serious. Moreover, depending on the nature and severity of the dendritics, it is quite possible for a unit (system) to contain several nonconformities and not be classified as nonconforming (Montgomery, 1996). For this reason, the weighted chart is a handy tool in cases of this sort.

As an example, suppose the manufactured items are personal computers. Each unit could have one or more very minor flaws in the cabinet finish and since these flaws do not seriously affect the unit's functional operation, it could be classified as conforming. However, if there are severe defects or too many of these flaws, the personal computer should be classified as nonconforming, since the flaws would be very

noticeable to the customer and might affect the sale of the unit. In addition, this chart is also assumed to be well modeled by a Poisson distribution. Mathematically, u is the total number of demerits in a sample divided by the sample size, which is equal for every subgroup:

$$u_i = \frac{D_i}{n} = \frac{\sum_{h=1}^n d_h}{n} \quad (3.16)$$

where

i is used as a subgroup or sample index.

n is the sample size, which represents the number of observations per subgroup.

D_i is the total number of demerits in sample i (m_i).

d_h is described in Equation 3.1 (Section 3.5).

Since u is a linear combination of independent Poisson random variables, it can be plotted on a control chart with the following parameters (Montgomery, 1996):

$$\text{Center Line} = \bar{u} = 100\bar{u}_A + 50\bar{u}_B + 10\bar{u}_C + \bar{u}_D \quad (3.17)$$

$$UCL = \bar{u} + 3\hat{\sigma}_u \quad (3.18)$$

$$LCL = \bar{u} - 3\hat{\sigma}_u \quad (3.19)$$

where

$$\hat{\sigma}_u = \left[(100)^2 \bar{u}_A + (50)^2 \bar{u}_B + (10)^2 \bar{u}_C + \bar{u}_D \right]^{1/2} \quad (3.20)$$

In the preceding equations, \bar{u}_A , \bar{u}_B , \bar{u}_C , and \bar{u}_D represent the average number of Class A, Class B, Class C, and Class D dendritics, respectively, per subgroup. These values are

obtained from the analysis of preliminary data, taken when the process is supposedly operating in control. For example, to find the value of \bar{u}_A , the following

$$\bar{u}_{iA} = \frac{\sum_{h=1}^n c_{hA}}{n} \quad (3.21)$$

$$\bar{u}_A = \frac{\sum_{i=1}^m \bar{u}_{iA}}{m} \quad (3.22)$$

where

h is used as an observation index.

c_{hA} is the number of defects (dendritics) occurred in observation h (n_h).

m is the number of subgroups or samples taken in the preliminary study.

3.7.5 EWMA Chart

The exponentially weighted moving average (EWMA) control chart is a good alternative to the Shewhart control chart when small shifts in the process mean, in the order of 1.5σ or less, need to be detected (Ng and Case, 1989). Like Shewhart control charts, the EWMA control chart is easy to implement and interpret (Lucas and Saccucci, 1990). Consider a process from which the sequence of quality measurements x_1, x_2, \dots, x_i is taken in each subgroup, assuming that x_1, x_2, \dots, x_i are i.i.d. Poisson random variables with mean μ . When the process is in control, $\mu = \mu_0$ (the specified or target value). To monitor the process, an EWMA chart can be applied. It is based on the subsequent statistic (Montgomery, 1996):

$$Z_i = \lambda x_i + (1 - \lambda)Z_{i-1} \quad (3.23)$$

The starting value, Z_o (required with the first sample at $i = 1$), is often taken to be the target value (μ_o). If μ_o is not known, the average of the subgroups in the preliminary samples is used as the starting value of the EWMA, so $Z_o = \bar{x}$; thus, $Z_o = \mu_o = \bar{x}$. The \bar{x} stands for any of the c , p or u Shewhart charts (\bar{c} , \bar{p} or \bar{u} , respectively). Likewise, the x_i in Equation 3.25 refers to the subgroup value of any of the c , p or u attribute control charts. This connotes that the EWMA chart is constructed based on the type of Shewhart (attribute) control chart selected. The process is considered to be out of control and action should be taken whenever Z_i falls outside the range of the control limits (Ng and Case, 1989). Therefore, the EWMA control chart would be constructed by plotting Z_i versus the sample number i . The center line and control limits for the EWMA control chart are as follows (Borror *et al.*, 1998):

$$UCL = \mu_o + L \sqrt{\frac{\lambda \mu_o}{2 - \lambda} [1 - (1 - \lambda)^{2i}]} \quad (3.24)$$

$$Center Line = \mu_o \quad (3.25)$$

$$LCL = \mu_o - L \sqrt{\frac{\lambda \mu_o}{2 - \lambda} [1 - (1 - \lambda)^{2i}]} \quad (3.26)$$

here,

i is used as a subgroup or sample index.

L is the distance of the control limits from the center line in multiples of the standard deviation (σ).

λ is the weighting factor (sometimes called weight).

The design factors of the EWMA control chart are L and λ which give the desired in-control ARL. The average run length (ARL) provides assistance in choosing what these two values should be worth. The ARL of a control charting procedure is defined as the expected number of sampling stages until an out of control condition is raised (Grant and Leavenworth, 1996). When a process is in control, a large ARL is desired. On the other hand, when a shift has occurred and it is necessary to detect the shift as quickly as possible it is desirable to have a small ARL for an out-of-control process (Borror *et al.*, 1998).

The ARL is used to determine the values for the factors of the EWMA control chart, L and λ . There have been several theoretical studies of the ARL properties of the EWMA control chart (Montgomery, 1996). These studies provide average run length tables or graphs for a range of values of L and λ . The average run length performance for several EWMA control schemes is shown in Table 3.2.

Table 3.2: Average run lengths for several EWMA control schemes (Lucas and Sacucci, 1990).

Shift in Mean multiple of σ	$L=1$	$L=2$	$L=3$	$L=4$	$L=5$
0	500	500	500	500	500
0.25	224	170	150	106	84.1
0.50	71.2	48.2	41.8	31.3	28.8
0.75	28.4	20.1	18.2	15.9	16.4
1.00	14.3	11.1	10.5	10.3	11.4
1.50	5.9	5.5	5.5	6.1	7.1
2.00	3.5	3.6	3.7	4.4	5.2
2.50	2.5	2.7	2.9	3.4	4.2
3.00	2.0	2.3	2.4	2.9	3.5
4.00	1.4	1.7	1.9	2.2	2.7

For example, suppose an in control ARL of 500 is desired (the control chart will plot 500 points before a “false alarm” out of control point is plotted); in Table 3.2, the various values for L and λ will give in control ARL's of 500. Additionally, it is also desired to detect a shift in the safety mean of 1.00 (one standard deviation, σ) above or below the control limits. Using the values for L and λ in column one, these numbers should be 3.054 and 0.40, respectively. Therefore, if the system is in control the ARL_0 is 500 and for detecting a variation in the process mean of 1σ the ARL_1 is 14.3 (it will take roughly 15 subgroups to detect the shift with a point outside of the control limits).

In general, values of λ in the interval $0.05 \leq \lambda \leq 0.25$ work well in practice, with $\lambda = 0.05$, $\lambda = 0.10$, and $\lambda = 0.20$ being popular choices (Montgomery, 1996). A good rule of thumb is to use smaller values of λ to detect smaller shifts. Further, $L = 3$ (the usual 3 sigma, 3σ , control limits) works reasonably well, particularly with the larger value of λ (0.40). However, when λ is small, $\lambda \leq 0.1$, there is an advantage in reducing the width of the limits by using a value of L between 2.6 and 2.8 approximately, according to Montgomery (1996).

It is important to point out that when constructing an EWMA chart in the PSMIS, the person first needs to select a type of Shewhart chart (c , p or u). The reason for this is because the control limits and the plotted points of the EWMA control chart are computed based on the center line and subgroup values, respectively, of the selected attribute chart. This means that the PSMIS creates a c , p or u based EWMA chart, depending on the analyst's selection. For instance, a c based EWMA control chart cannot be plotted using the center line and sample values from the p or u chart. The c based

EWMA chart has to be created using the using the mean and subgroup values of the c control chart, like comparing apples with apples and oranges with oranges. Moreover, in order to define the control limits for the EWMA chart, the PSMIS will ask the user to indicate the L and λ factors, (notice Figure 3.22). The values of these factors are depicted in Table 3.2. The software program has a help option that provides suggestions to the analyst about commonly used values for these factors.

3.7.6 Combined Shewhart—EWMA Control Chart

As mentioned earlier, the EWMA performs well detecting small shifts but does not react to large shifts as quickly as the Shewhart control chart. A good way to further improve the sensitivity of the control procedure to large shifts without sacrificing the ability to detect small shifts quickly is to combine a Shewhart control chart with the EWMA (Borrer *et al.*, 1998). The combined Shewhart-EWMA control procedure is effective against both large and small shifts. This refers that it is possible to plot both the Shewhart chart and the EWMA chart on the same graph along with the associated control limits for each chart (Hunter, 1986). This produces one chart for the combined control procedure which analysts quickly become adept at interpreting.

Of course, the use of either the Shewhart control charts or the EWMA control chart, or both, in CHTFPM depends upon the nature of the system being analyzed and the desired protection from unwanted risks and hazards. If the system under observation has a good track record regarding safety and is relatively stable then, for simplicity, one of

the Shewhart control charts described before will suffice. However, if small shifts in the overall safety mean cause system safety to degrade to unacceptable levels, the EWMA control chart should be used. It is recommended that if detecting small and large shifts is desirable, both the Shewhart and EWMA control chart should be used concurrently.

3.8 Decision Support Structure of the PSMIS

The CHTFPM MIS aids the system analyst in making decisions when dealing with especial issues in a given system or process. These unique subjects are given below:

- Points out-of-control
- Outliers
- Assignable causes
- Trend analysis
- Pattern recognition

It is important to highlight at this point in time that most of the whole process of creating a project is iterative. This denotes that the user can update, change or erase previous information (wherever the PSMIS allows it) at any moment; consequently, the results previously calculated will be recomputed or changed. Most important, although the PSMIS offers recommendations to the system evaluator, the analyst can choose to do whatever he/she deems more convenient or appropriate.

If a plotted point in a control chart is outside the control limits (out of control), the system assessor can trace that observation to investigate the reason of that matter. If the analyst finds out that the cause of such outcome is insignificant, then the person can treat

that observation point as an outlier, which means that the process or system is not becoming hazardous. If this is the case, the PSMIS will suggest the user to erase the information (recorded dendritic occurrences) in that particular subgroup and continue using the same control limits for future samples.

On the contrary, if that same point turns out to be an assignable cause (dendritic) that can jeopardize the safety integrity of the system, then the system evaluator has to take corrective action to fix the problem that caused such hazardous condition. Once the fault has been repaired, the analyst should re-establish the control chart parameters: center line, UCL and LCL. That is, new control limits must be employed since the process is no longer operating under the presence of hazards.

This connotes that the same procedure followed to obtain the control boundaries for the first time must be repeated. This denotes that the previous points will not be plotted in the control chart with the new control parameters. For this reason, the PSMIS will propose the user to create a new project in order to preserve the previously documented data. To avoid re-typing the same information of the original study, the user can duplicate the first project and save the new one with a different name , and he or she will just have to delete the observed dendritics that were registered in the sampling sheets. After that, the analyst can use the same preliminary sampling plan as the first one (original) or create a new one and begin the process of conducting preliminary samples to establish the new control limits. Once this has been done, the user can proceed to perform the actual sampling, which will have the latest control limits obtained from the recent preliminary data set.

Trending and pattern recognition are insightful tools to make inferences on the safety status of the system under observation. These methods provide the data source for predictive safety. These approaches are the most common used for data evaluation when applying condition monitoring. The failure information associated with a system is used to supply the limits that the trend and pattern recognition will be measured against and what can be called an alarm limit value (Dicquemare, 1997).

If the points in a control chart are truly random, an even distribution of the points is expected above and below the centerline. However, a control chart may indicate an out-of-control condition either when one or more points fall beyond the control limits or when the plotted points exhibit some nonrandom pattern or peculiar behavior, as shown in Figure 3.20.

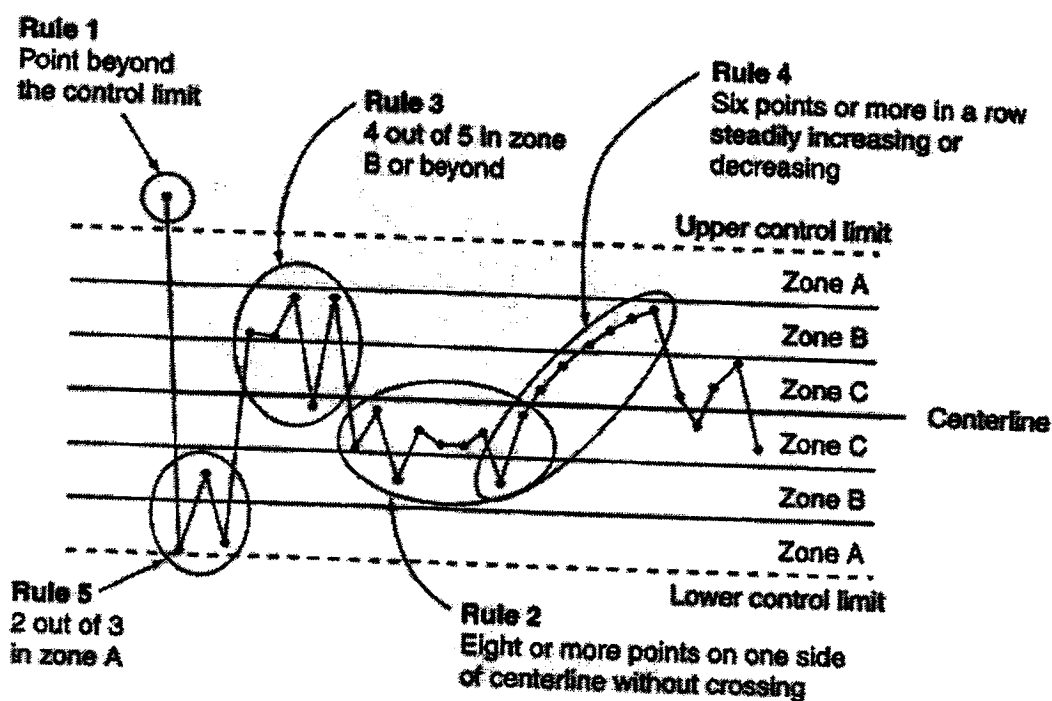


Figure 3.20: Assignable cause patterns on a control chart (Wise and Fair, 1998)

The PSMIS will prompt the analyst to consider the following simple rules recommended by Wise and Fair (1998) to recognize or detect an out-of-control condition; hence, take corrective and preventative measures:

1. Points beyond the control limits.
2. Eight or more consecutive points either above or below the center line.
3. Four out of five consecutive points in or beyond the 2σ limits (referred to in Figure 3.20 as Zone B).
4. Six points or more in a row steadily increasing or decreasing.
5. Two out of three consecutive points in the 3σ region (referred to in Figure 3.20 as Zone A).

3.8.1 Management Reports of the PSMIS

The management reports are generated from all the information that was included in the project. In other words, the PHA, FMEA, barrier analysis, dendritic list, control charts, *etc.* can be viewed in a defined format or in the form of a report. Since everything was already calculated (UCL, LCL, dendritics frequency, *etc.*) by the CHTFPM code, the program easily extracts the requested information and displays it in a report fashion, which can be printed or viewed on the screen. Figures 3.21 and 3.22 illustrate the flowchart of this process.

Additionally, to display the control charts, the individual has to indicate which chart to view: Shewhart, EWMA or the combined Shewhart-EWMA control chart, as

depicted in Figure 3.22. Furthermore, the end-user can copy the tables, charts or diagrams and paste them in a different file or document.

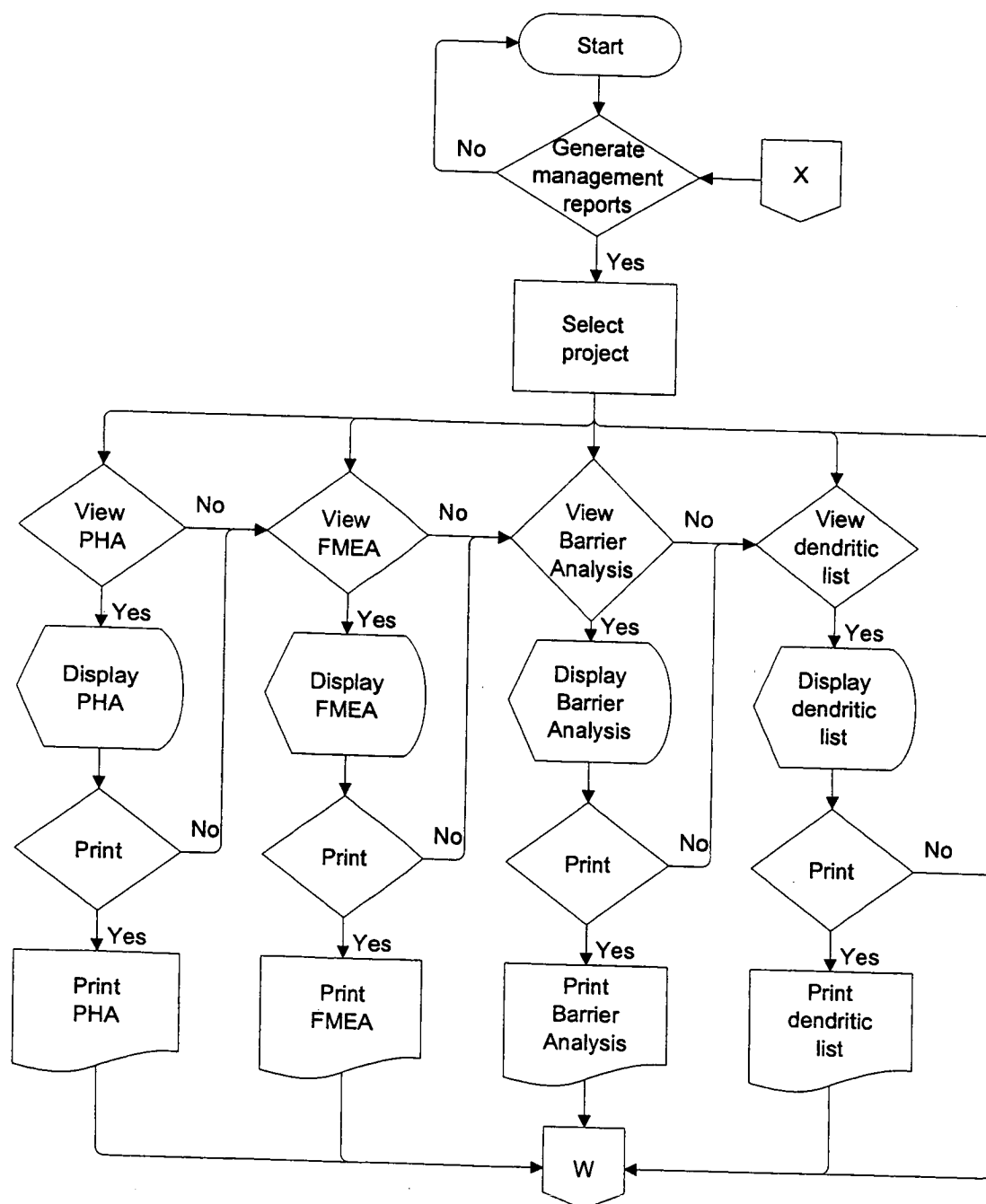


Figure 3.21: Flowchart of management reports (part 1).

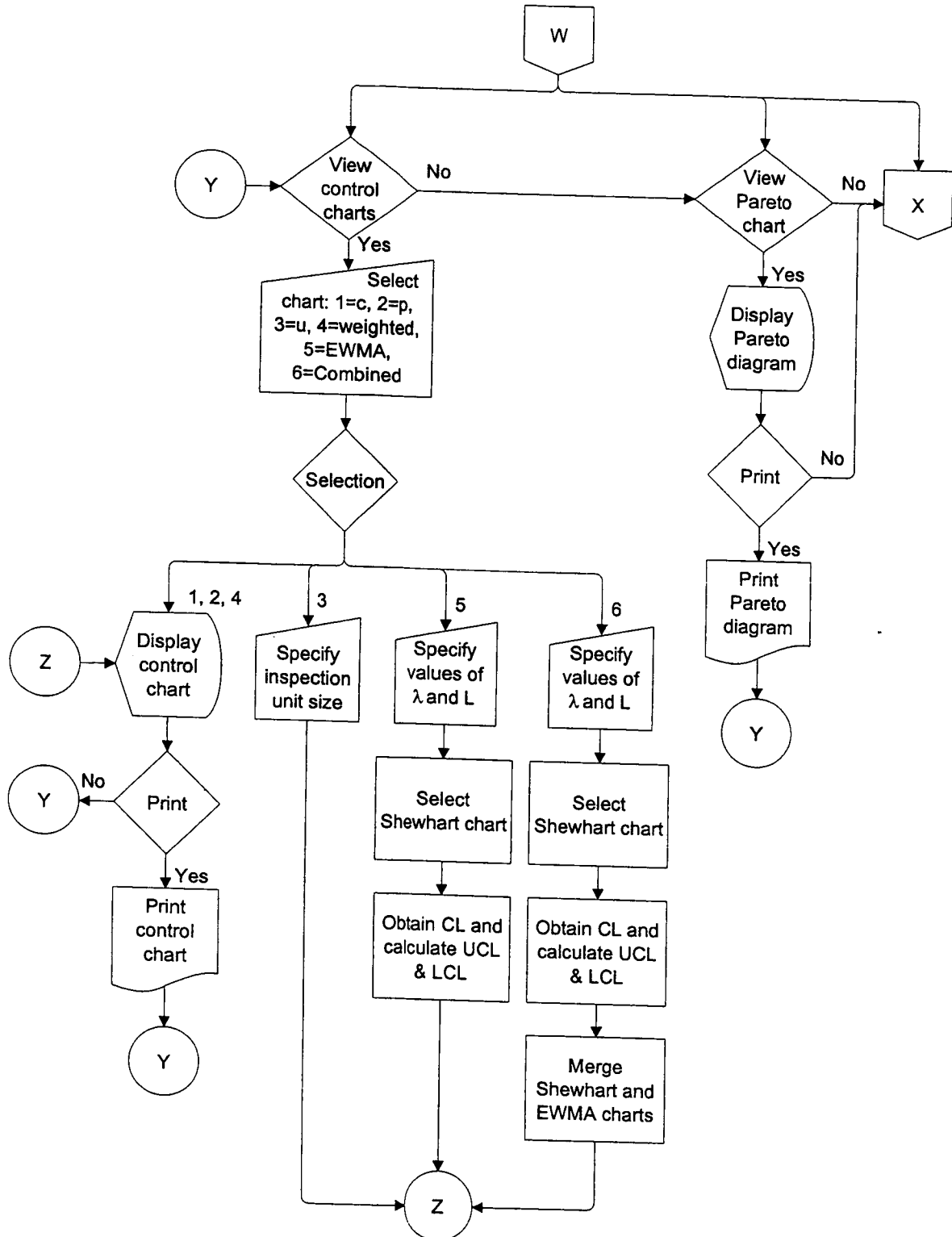


Figure 3.22: Flowchart of management reports (part 2).

Some parts of the project elaboration, as it was said just earlier, are iterative; therefore, the analyst can make the permitted changes to a project at any point. If this happens, the existing results associated with the new modifications will be affected accordingly, but the software application will warn the analyst with regards to the alterations that are about to take place and will prompt him/her for its consent. If the individual retracts from its choice, then the changes will not be saved and the current information will remain the same.

A useful feature of the PSMIS is that it offers the user the ability to view the collected data in any type of Shewhart control chart if he or she wants to as it is notice in Figures 3.21 and 3.22. Nevertheless, to realize this operation, the system analyst needs to go back to the point where the control limits are established, specifically where the person selects the type of attribute chart (observe Figure 3.17). To return or go to a locality of interest in the program, the user can simply click on the respective buttons to continue or advance in the project process until it arrives to the desired location.

3.8.2 Help Screens and Decision Support

The PSMIS will aid or guide the user on how to fill out forms and fields by providing assistance and advice through help screens. The sections contained in this chapter include explanations and suggestions to perform certain tasks in the computer program. All those clarifications or steps that describe how to utilize a function of the software are summarized in help windows, which are available to the analyst. Many of these help dialogue boxes are recommendations to the end-user, so that optimum results

can be obtained, like in the case of deciding what type of control chart to use. In this situation the CHTFPM MIS will offer the user the references explained in Table 3.3 in the form of a help screen that would be accessible to the system analyst. However, the individual always has the liberty of taking the course of action that is more convenient based on the desired results, system being considered and personal judgment.

Table 3.3: Summary of control chart applications in the CHTFPM (Quintana *et al.*, 2001).

Control Chart	Definition	Strengths	Weaknesses	Applicability to CHTFPM
<i>p</i> control chart	Ratio of nonconforming items in a population to the total number of items in that population	Relative ease of implementation, calculations, and easy to explain	Does not detect small shifts ($<1.5\sigma$) well	Use to describe dendritic frequency in relation to maximum possible occurrences
<i>c</i> control chart	Counts the total number of nonconformities in a unit or inspection sample	Relative ease of implementation, calculations, and easy to explain	Does not detect small shifts ($<1.5\sigma$) well	Use when a count of dendritics is desired
<i>u</i> control chart	Tracks the average number of nonconformities per unit	Relative ease of implementation, calculations, and easy to explain	Does not detect small shifts ($<1.5\sigma$) well	Use when the sample size is not constant
Weighted <i>c</i> control chart	Classifies defects according to seriousness	Signals according to severest dendritics	Incorrect classification of defect could cause false alarms	Applicable when some dendritics are more important than others
EWMA control chart	Use when detecting small shifts (1.5σ or less) is desired	Detects small shifts better than Shewhart control charts	Does not detect large shifts as well as Shewhart control charts	Applicable when small shifts in the safety mean raise unacceptable safety risks
Combined Shewhart-EWMA control chart	Use when both small and large shifts need to be detected	Provides analysis to detect both large and small shifts	Short time period necessary for analyst to become adept at interpreting chart	Use if EWMA control chart is being used to detect small shifts

The PSMIS not only provides warnings to the analyst in order to prevent mistakes, but is also offers the user recommendations in decision making so that he or she

can understand and interpret the results without difficulty. For instance, the CHTFPM MIS offers the user suggestions about which control chart or distribution is more suitable for the type of data collected, as the ones described in Table 3.3 which elucidates the appropriateness of each control chart and its recommended application(s). The software package does this by means of informing the user what kind of control chart is more convenient according to the response being sought. It is up to the system assessor to determine which control chart would be most advantageous to implement depending on the circumstances of the system.

An important aid that the PSMIS provides to the user is when an inspection or observation screen—where the dendritic occurrences are typed in—is not filled out on purpose maybe because no dendritics occurred. When this happens, the PSMIS/CHTFPM MIS will assume that such observation was not conducted and will affect the subgroup size, hence various calculations and results. In spite of this, the CHTFPM MIS will prevent the person from committing such mistake by alert him/her that there are some blank observations. Additionally, the warning message will say how to avoid this problem. It will tell the user to simply place a 0 (zero) in any of the boxes that are next to every dendritic in the observation window that was empty. By doing this, the software program will know that no dendritics were observed in that specific inspection and will count that observation toward the necessary computations.

If an observation number (screen) was skipped or not filled in either intentionally or accidentally, the PSMIS will notify the analyst of this issue by displaying the message box previously mentioned. Nonetheless, the user can choose to leave unfilled such

inspection number. If this is the case, the CHTFPM computer system will inform the user with a second warning message that the only available control chart will be \bar{x} chart because the subgroups vary in sample size. In other words, to view the control charts other than the \bar{x} chart, the size of each subgroup have to be the same (review Section 3.7 entirely for sample size restriction). If the analyst does not want to be restricted only to the \bar{x} control chart, then the vacant observation screens have to be filled out.

Chapter 4

4. IMPLEMENTATION AND EVALUATION OF THE PSMIS

This chapter describes the implementation as well as the evaluation of the PSMIS or CHTFPM MIS. As was explained in Section 1.5, two previously NASA validated projects served as the platform to implement the PSMIS. The results from those two predictive safety studies were compared with the outcomes obtained using the CHTFPM MIS to determine the reliability of the results given by the software application.

Moreover, the time and the manpower (persons) required to finish each study manually was measured against the time and manpower necessary to complete those same projects when the CHTFPM computer program was utilized. Therefore, to evaluate the reliability and efficiency of this predictive safety software package, three key factors were considered: accuracy of results as well as manpower and time, respectively.

4.1 Introduction

The implementation and evaluation of the PSMIS is outlined in Section 4.2, while Section 4.3 provides a point by point comparison of the construction of dendritics among the manual and PSMIS approach. Section 4.4 describes the creation of the sampling sheet from the manual and PSMIS perspective. In Section 4.5, the development of the sampling plan in the PSMIS is elucidated, followed by Section 4.6 that reveals how the PSMIS

depicts the statistical significance for a project. Section 4.7 presents the types of charts created by the PSMIS, and Section 4.8 shows the reliability and efficiency of the PSMIS.

4.2 Implementation and Evaluation Synopsis of the PSMIS

The implementation and evaluation of the PSMIS can be summarized in the following steps:

1. Development of dendritic elements.
2. Design sampling sheet.
3. Determine rational subgroups, sample size, and sampling plan.
4. Demonstrate statistical significance.
5. Establish control limits and control charts.
6. Attest reliability and efficiency of the PSMIS.

The above steps were used to carry out the implementation of the CHTFPM MIS or PSMIS using the selected case studies (see Section 1.5). The systems under consideration were the promoted combustion testing chamber at the Marshall Space Flight Center (MSFC) and the hoisting operation of four high-pressure gas tanks (HPGTs) at Kennedy Space Center (KSC).

The hazards involved in the promoted combustion testing are several. For instance, heavy parts of the test apparatus are moved on a regular basis by the operators and if not handled with caution, it could cause an injury (*e.g.* foot injury if a heavy component falls on top of the operator's foot). Testing involves burning materials in an oxygen-enriched environment, thus introducing the hazards associated with explosions.

There could be a burn hazard to the operator that could occur during sample unloading because of molten metal slag. Sample preparation technicians frequently handle cleaning solvents that require personal protective equipment.

Similarly, the hoisting operation and testing of the HPGTs at KSC entails hazards related to cumulative trauma disorders such as back or shoulder injuries due to reaching when hoisting the tanks. In addition, the operators work with pressurized gas cylinders containing oxygen and nitrogen, so if personnel mishandles or leans heavily on the tanks, it could release an explosion. Hence, workers are exposed to numerous hazards of different kinds.

The CHTFPM MIS has two basic features, which are namely the construction of dendritics, which originate the hazards, of a system and the development of the sampling study to be conducted in order to detect the presence those dendritics. Based on these two qualities, the procedure for implementation of the CHTFPM MIS is described in the following sections which are elaborated using the case studies described in Section 1.5.

4.3 Development of Dendritic Elements

The dendritics for the promoted combustion testing operations at MSFC as well as the dendritic elements for the testing, preparation and hoisting operation of the HPGTs at KSC are developed in the following subsections. Determination of the conditions leading to hazards, the dendritics, is a major step in the development of a project in the PSMIS.

The dendritic focus is on human interaction with the system, as it pertains to both industrial scenarios. Consultation with system engineers and operators, allowed for the


refinement of hazard criterion. Understanding the substructure of the systems under study is essential to recognize possible hazards, thus allowed for the inception of dendritic construction, namely the preliminary hazard analysis.

4.3.1 Preliminary Hazard Analysis

Dendritics are built in part by the fabrication of the Preliminary Hazard Analysis (PHA), which aids the analyst in identifying and evaluating hazards as well as the safety design and operations requirements needed to maintain system safety. The PHA is performed to provide an initial risk assessment of a system. It is based on the best available data, including mishap data from similar systems. Design controls and other actions needed to eliminate or control the hazard(s) should be considered or documented.

Hazardous Condition	Hazard Cause	Hazard Effect	Safety/Engineering Requirements	Hazard Elimination/Control Provisions
Expired calibration (gauge, transducer, etc.)	Human error (scheduling)	Loss of confidence in component indication	Meet minimum calibration requirements as specified by manufacturer	Calibration schedule reviews and audits

(a)

Preliminary Hazard Analysis				
Project ID <input type="text" value="MIKEC"/>		Date <input type="text" value="Tuesday, May 13, 2003"/>		Description <input type="text" value="The system is the promoted combustion testing chamber at the Material Combustion Research Facility located on Marshall Space Flight Center."/> 
Project name <input type="text" value="Promoted Combustion Testing"/>				
Analyst name <input type="text" value="Michael Camet"/>				
Hazardous Condition	Hazard Cause	Hazard Effect	Safety/Engineering Requirements	Hazard Elimination/Control Provisions
Expired Calibration (gauge, transducer, etc.)	Human error (scheduling).	Loss of confidence in component indication.	Meet minimum calibration requirements as specified by manufacturer.	Calibration schedule reviews and audits.
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

(b)

Figure 4.1: Comparison between the (a) manual and (b) PSMIS approach for the PHA forms of the MSPC case study.

Two PHAs were performed manually, one for the MSFC study (Appendix A shows the entire PHA of this project) and the other for the KSC case scenario (see Appendix H for the entire PHA of this project). Additionally, the corresponding PHAs were built using the PSMIS. Figure 4.1 depicts the comparison between a portion of the resulting PHA for the MSFC project by applying the two approaches: manually and via CHTFPM MIS. In the same way, Figure 4.2 portrays the contrast among two segments of the PHA, accordingly, for the KSC study.

Hazardous Conditions	Hazard Cause	Hazard Effect	Safety/ Engineering Requirements	Hazard Elimination Control Provisions
1. Non-hazard proof electrical equipment	Human Error (Failure to follow SOP)	Fire/Explosion resulting in injury or death to personal and loss of or damage to flight hardware, Ground Support Equipment (GSE), and facility.	Lock out and tag out all non-hazard proof non-electrical equipment	High Pressure Gas Tanks test work authorization procedures (WAP) contain steps requiring a walk down to verify that all electrical equipment has been locked out and tagged.

(a)

Preliminary Hazard Analysis				
Project ID: <input type="text" value="SPROJ"/>		Date: <input type="text" value="Tuesday, May 13, 2003"/>		Description: <input type="text" value="The Application of a Continuous Hazard Tracking and Failure Prediction Methodology."/> <input type="button" value="Go to PMEA"/>
Project name: <input type="text" value="Senior Project"/>				
Analyst name: <input type="text" value="Javier Avalos"/>				
Hazardous Condition	Hazard Cause	Hazard Effect	Safety/Engineering Requirements	Hazard Elimination/Control Provisions
1. Non-hazard proof electrical equipment	Human Error (Failure to follow SOP)	Fire/Explosion resulting in injury or death to personal and loss of or damage to	Lock out and tag out all non-hazard proof non-electrical equipment	High Pressure Gas Tanks test work authorization procedures (WAP) contain

(b)

Figure 4.2: Comparison between the (a) manual and (b) PSMIS approach for the PHA forms of the KSC case study.

Notice how the two PHAs done by hand (using a word processor program) vary in format; this is because the analysts involved in the distinct projects have dissimilar

interests or appeals. On the contrary, the PHAs created by the PSMIS have consistency throughout. Furthermore, the portions of the PHAs of the two studies are exact replicas of the original analyses forms; this signifies that no modifications have been made to their appearance at the time of copying them to this project. This is also the case for the FMEA and barrier analysis which are presented next.

4.3.2 Failure Mode and Effect Analysis

The PHA, by granting a basic depiction of the hazards and the subsequent safety design criterion thereof, facilitates the second tool used in dendritic derivation: the failure mode and effect analysis (FMEA). The FMEA is constructed based on the results obtained in the PHA. The FMEA is defined as a bottom-up method of identifying the failure modes of a system and determining the effects on the next higher level. Thereby the FMEA form in the PSMIS contains, among others, three fields (or boxes) entitled “Local Effects,” “Next Higher Level,” and “End Effects” since there can be more than one effect caused by a failure. The derived FMEAs (for both projects) consider human/machine interaction and the possible consequences of such interaction

It is important to mention that there are several techniques to construct an FMEA, but they are all similar in the sense that they include the same essential information (fields or headings). Basically, the only variation among the various techniques is that the titles of the fields are arranged in a distinct way. The following figures show fractions of the FMEA for both the MSFC and KSC safety studies with their respective FMEA forms created by the CHTFPM MIS (Appendix B and I give the full FMEA for the MSFC and

KSC project, respectively). The FMEA for the MSFC case study is different from the one for the KSC industrial scenario; moreover, these two FMEA forms are dissimilar from the one that the PSMIS utilizes. Therefore, Figures 4.3 and 4.4 illustrate the distinctions between three types of FMEA forms. However, it is fundamental to remember that the FMEAs of each project are an identical copy of the original analyses.

Find No. / Part No.	Part Name	Part Function	FAILURE MODE B. CAUSE FAILURE MODE NUMBER D. INSPECTION / RECORD E. VARYING G. yet to be determined	Failure Effects on System Performance	Failure Effects on Systems and/or Personnel Safety	3
N/A	Calibration Technician	Performs calibration of assigned equipment (gauges, transducers, etc)	A. Fails to calibrate equipment by due date B. Scheduling D. Inspection of calibration records, visible discrepancy in equipment, etc... E. Calibrate F. Varying G. yet to be determined	<input type="checkbox"/> Loss of confidence in equipment indication / operation <input type="checkbox"/> Possible failure cause in function / use / operation of equipment or system <input type="checkbox"/> Possible factor in equipment downtime and/or life expectancy	Possible effects include minor to severe personnel risks, system component failure, system failure	3

(a)

Failure Mode Effect Analysis						
Go to PHA	Project ID: MIKEC	Date: Tuesday, May 13, 2003	Description: The system is the promoted combustion testing chamber at the Material Combustion Research Facility located on Marshall Space Flight Center.			
	Project name: Promoted Combustion Testing					
	Analyst name: Michael Camet					
Go to Barrier Analysis						
Failure Mode / Failure Cause	Operational Phase	Local Effects	Next Higher Level	End Effects	Fault Detection	Compensating Provisions
Failure to calibrate equipment by due date / scheduling.	Calibration technician performs calibration of	Loss of confidence in equipment indication / operation	Possible failure cause in function / use / operation of equipment or	Possible effects include minor to severe personnel risks / system	Inspection of calibration records, visible discrepancy in	Calibrate

(b)

Figure 4.3: Comparison between the (a) manual and (b) PSMIS approach for the FMEA forms of the MSFC case study.

In some boxes, which are the fields, of the FMEA forms created by the CHTFPM MIS, the text does not fully fit or is not completely visible. Nonetheless, each box has a

scroll bar that appears in the field when the cursor is in it, thus enabling the user to view the entire comment in that area or topic.

Tubing / Transport Oxygen from PRUA to HPGT	Ignition	Fire/Explosion resulting in injury or death to personal and loss of or damage to flight hardware, Ground Support Equipment (GSE), and facility.	Striking a valve body just downstream of the control element of the valve can cause Particulate Impact ignition caused by the exposure of un-oxidized metal surfaces.	Five 10 Micron filters remove particulates.	Continue to use five 10 Micron filters remove particulates.
---	----------	---	---	---	---

(a)

Failure Mode Effect Analysis						
Project ID: SPROJ		Date: Tuesday, May 13, 2003		Description: The Application of a Continuous Hazard Tracking and Failure Prediction Methodology.		
Project name: Senior Project						
Analyst name: Javier Avalos						
Go to PHA						Go to Barrier Analysis
Failure Mode / Failure Cause	Operational Phase	Local Effects	Next Higher Level	End Effects	Fault Detection	Compensating Provisions
Ignition / Striking a valve body just downstream of the control element of	Tubing / Transport Oxygen from PRUA to HPGT	Fire / Explosion	Injury or death to personnel	Loss or damage to flight hardware, Ground Support Equipment (GSE)	Five 10 Micron filters remove particulates.	Continue to use five 10 Micron filters remove particulates.

(b)

Figure 4.4: Comparison between the (a) manual and (b) PSMIS approach for the FMEA forms of the KSC case study.

It can be clearly seen that the FMEAs produced by the PSMIS are not precise duplicates of the manual forms, as it was explained earlier. However, the same information contained in the original FMEAs is also comprised in the FMEA forms developed by the PSMIS, respectively. This is particularly true because the same topics, hence the same information, are incorporated in the FMEA forms of the CHTFPM MIS,

correspondingly. The slight disparity is just in the order or fashion that the fields are structured in each type of FMEA.

4.3.3 Barrier Analysis

The two complete barrier analyses for the MSFC and KSC case studies are depicted in Appendix C and J, correspondingly. The barrier analyses were performed on several hazards not identified on the PHA and on the FMEA. Especially those hazards pertaining to humans were included in these analyses since this type of analysis works exceptionally well when analyzing human factors affecting system safety or system components jeopardizing human safety. Again, a section of the barrier analyses of both projects are shown along with their concomitant PSMIS analyses forms in Figure 4.5 and 4.6 for the MSFC and KSC project, respectively.

Personnel	Back Injury	Training on general safe lab practices	Incorrect posture used
-----------	-------------	---	---------------------------

(a)

Barrier Analysis

<div style="background-color: black; color: white; padding: 2px; text-align: center;">Go to FMEA</div>	Project ID: <input type="text" value="MIKEC"/> Date: <input type="text" value="Tuesday, May 13, 2003"/> Project name: <input type="text" value="Promoted Combustion Testing"/> Analyst name: <input type="text" value="Michael Canet"/>	Description: <input style="width: 90%;" type="text" value="The system is the promoted combustion testing chamber at the Material Combustion Research Facility located on Marshall Space Flight Center."/>	<div style="background-color: black; color: white; padding: 2px; text-align: center;">Go to Dendritics</div>
--	---	---	--

Target	Thread	Barrier	Analysis
Personnel	Back Injury	Training on general safe lab practices.	Incorrect posture used.

(b)

Figure 4.5: Comparison between the (a) manual and (b) PSMIS approach for the barrier analysis forms of the MSFC case study.

All personnel exposed to GOX leaks shall remain isolated from ignition sources for at least 30 min.	Human Barrier	Human Failure
---	---------------	---------------

(a)

Barrier Analysis				
Go to FMEA	Project ID	SPROJ	Date	Tuesday, May 13, 2003
	Project name	Senior Project		
	Analyst name	Javier Avalos		
		Description	The Application of a Continuous Hazard Tracking and Failure Prediction Methodology.	
		Go to Dendritics		
Target	Thread	Barrier	Analysis	
Personnel	Ignition	All personnel exposed to GOX leaks shall remain isolated from ignition sources for at least 30 min.	Human Failure	

(b)

Figure 4.6: Comparison between the (a) manual and (b) PSMIS approach for the barrier analysis forms of the KSC case study.

4.3.4 Dendritic Construction

The last step in the construction of dendritics consists of using the completed PHA, FMEA and barrier analysis to obtain a final list of conditions that may become hazardous. These conditions are known as dendritic elements or just dendritics. After reviewing each item in the PHA, FMEA and the barrier analysis, a preliminary dendritic list was formed depicting possible occurrences that may result in system failure or accidents. Afterward, the list is revised to check for any repeating or similar elements and to rephrase any items if necessary in order to arrive to the final list of dendritics. The dendritic roster is a useful tool that allows system personnel to determine the behaviors/actions that could cause potential hazards, which could lead to accidents or failures, in the future. Figures 4.7 and 4.8 represent a portion of the dendritic roll for the

MSFC and KSC case studies, respectively, in comparison with the lists made by the CHTFPM MIS, accordingly. Refer to Table 4.1 and Appendix K for the whole dendritic list of the MSFC and KSC project, correspondingly.

Dendritic List	
1.	Failure to adhere to SOP
2.	Incorrect procedure used to don latex gloves
3.	Same surface contact (bare hand and glove)
4.	Personnel wearing dirty latex gloves
5.	Trash and combustibles not in fire retardant containers
6.	Test area not in "limited access control"
7.	Test cell used for storage
8.	Personnel limitations for a test cell exceeded (maximum of five)
9.	Personnel not wearing safety shoes in test area or while moving heavy objects

(a)

Dendritics List		
Project Number:	MIKEC	Date: Tuesday, May 13, 2003
Project Name:	Promoted Combustion Testng	
Description:	The system is the promoted combustion testing chamber at the Material Combustion Research Facility located on Marshall Space Flight Center.	
Analist:	Michael Camet	
Create/Reset Dendritics		
ID	Dendritic	Weight
1	Failure to adhere to SOP	100
2	Incorrect procedure used to don latex gloves	50
3	Same surface contact (bare hand and glove)	50
4	Personnel wearing dirty latex gloves	50
5	Trash and combustibles not in fire retardant containers	1
6	Test area not in "limited access control"	10
7	Test cell used for storage	1
8	Personnel limitations for a test cell exceeded (maximum of five)	1
9	Personnel not wearing safety shoes in test area or while moving heavy objects	10

(b)

Figure 4.7: Comparison between the (a) manual and (b) PSMIS dendritic list of the MSFC case study.

1	Protective coverings askew/leaking/corroded.
2	Instrumentation calibration not done on regular scheduled intervals.
3	Hose/tubing in high-traffic area.
4	Personnel not wearing proper Personal Protective Equipment.
5	Over pressurization of HPGTs.
6	Under pressurization of HPGTs.
7	Flow rates exceed preset limits.
8	Temperature exceeds preset limits.
9	General cleanliness.

(a)

Dendritics List		
Project Number:	SPROJ	Date: Tuesday, May 13, 2003
Project Name:	Senior Project	
Description:	The Application of a Continuous Hazard Tracking and Failure Prediction Methodology.	
Analyst:	Javier Ayalos	
<input type="button" value="Create/Reset Dendritics"/>		

ID	Dendritic	Weight
1	Protective coverings askew / leaking / corroded.	100
2	Instrumentation calibration not done on regular scheduled inte	50
3	Hose / tubing in high-traffic area.	10
4	Personnel not wearing proper Personal Protective Equipment.	1
5	Over pressurization of HPGTs.	100
6	Under pressurization of HPGTs.	50
7	Flow rates exceed preset limits.	50
8	Temperature exceeds preset limits.	100
9	General cleanliness	50

(b)

Figure 4.8: Comparison between the (a) manual and (b) PSMIS dendritic list of the KSC case study.

The PSMIS creates the dendritic list automatically by pressing the “Import Dendritics” button (see Section 3.5). Additionally, the dendritic list form also has a scroll bar to view the whole roster of dendritics if they are not visible in the space provided.

Sampling Sheet

Project: MIKEC	Analyst: Michael Canet	Project's Date: 14-May-03
Name: Promoted Combustion Testing Operations		
Description: Promoted combustion testing chamber is located in the Materials Combustion Research Facility at Marshall Space Flight Center (MSFC).		

Group 1

Subgroup 1, 7:00:00 AM - 8:00:00 AM

7:08 AM Observation Number 1

Dendritic

	Weight	Occurrence
1 Failure to adhere to the SOP	100	<input type="text"/>
2 Incorrect procedure used to don latex gloves	50	<input type="text"/>
3 Same surfaces contacted (bare hand and latex glove)	50	<input type="text"/>
4 Personnel wearing dirty latex gloves	50	<input type="text"/>
5 Trash and combustibles not in fire retardant	1	<input type="text"/>
6 Test area not in "limited access control"	10	<input type="text"/>
7 Test cell used for storage	1	<input type="text"/>
8 Personnel limitations for a test cell exceeded	1	<input type="text"/>
9 Personnel not wearing safety shoes in test area	10	<input type="text"/>

Comments:

Wednesday, May 14, 2003

Page 1 of 20

Figure 4.10: Sampling sheet developed by the PSMIS for the MSFC project.

In the sampling sheet for the MSFC study that was done manually, the analyst is required to note down the time and day when the observation(s) was conducted. On the contrary, the sampling sheet elaborated by the PSMIS (Figure 4.10) includes the date when it was printed and the time when the observation should be conducted, so the analyst does not have to record such information. Therefore, it is strongly recommended to conduct the necessary observations on the same day the sampling sheet was printed, so that the printed date will match the observation date.

Similarly, in the sampling sheet for the KSC research study, the system evaluator has to write down the day and time when the observation will be conducted. Furthermore, this sampling form (Figure 4.11) does not have a space for commentaries, while the survey sheet constructed by the CHTFPM MIS (Figure 4.12) does incorporate an area for comments at the bottom of the page.

Date:		Times					
General/All Areas							
1	Protective coverings askew/leaking/corroded.						
2	Instrumentation calibration not done on regular scheduled intervals.						
3	Hose/tubing in high-traffic area.						
4	Personnel not wearing proper Personal Protective Equipment.						
5	Over pressurization of HPGTs.						
6	Under pressurization of HPGTs.						
7	Flow rates exceed preset limits.						
8	Temperature exceeds preset limits.						
9	General cleanliness.						

Figure 4.11: Sampling sheet created manually for the KSC project.

Sampling Sheet

Project: SPROJ	Analyst: Javier Avalos	Project's Date: 15-May-03
Name: Senior Project		
Description: The Application of a Continuous Hazard Tracking Failure Prediction Methodology.		

Group 1

Subgroup 1, 8:00:00 AM - 9:00:00 AM

8:13 AM Observation Number 1			
Dendritic		Weight	Occurrence
1	Incorrect procedure used to don latex gloves	100	<input type="text"/>
2	Instrumentation calibration not done on regular	50	<input type="text"/>
3	Hose/tubing in high-traffic area	10	<input type="text"/>
4	Personnel not wearing proper Personal Protective	1	<input type="text"/>
5	Over pressurization of HP GTs	100	<input type="text"/>
6	Under pressurization of HP GTs	50	<input type="text"/>
7	Flowrates exceed preset limits	50	<input type="text"/>
8	Temperature exceeds preset limits	100	<input type="text"/>
9	General cleanliness	50	<input type="text"/>

Comments:

Thursday, May 15, 2003

Page 1 of 8

Figure 4.12: Sampling sheet developed by the PSMIS for the KSC project.

4.5 Rational Subgroups, Sample Size and Sampling Plan

According to the rationale presented in Section 3.6.1, time order was the logical basis for the data collection in the two studies used to implement the PSMIS. The promoted combustion testing operations were videotaped over the period of a week. The videotaped operations were split into 100 subgroups with 4 observations in each subgroup. Therefore, the sampling plan for this case scenario (MSFC) was constituted by 100 samples of size 4, for a total of 400 observations. The random times corresponding to the necessary observations for the sampling scheme were generated using a random timer connected to a time lapse VCR (GYJR, Model Number TLC3168HD).

The mode in which this partition of subgroups was accomplished is described as follows. The videotaped operations were played back as input into the time lapse VCR. A random timer that randomly records a set number of clips of certain duration controls the time lapse VCR. The total time of the videotaped operations was split into 100 subgroups. The random timer was then set to randomly record 4 inspections from each subgroup. Each random inspection was approximately 10 seconds long to allow adequate time to check for all 21 dendritics.

On the other hand, the method that the PSMIS uses to achieve the separation of subgroups is by requesting the user to specify the number of groups, subgroups and observations per subgroup (see Section 3.6.3 for more details). Before setting up the sampling scheme, it is critical to keep in mind that the CHTFPM MIS first asks the user to develop a preliminary sampling plan (see also Section 3.6.3). In the MSFC project, the preliminary sampling scheme was composed of 10 samples (subgroups), which entailed

preliminary sampling scheme was composed of 10 samples (subgroups), which entailed 40 inspections, as seen in Figure 4.13. The preliminary observations are used to establish the center line and control limits for the Shewhart charts.

Set Preliminary Sampling Plan		
Number of groups:	<input type="text" value="1"/>	<input type="button" value="OK"/>
Number of subgroups per group:	<input type="text" value="10"/>	<input type="button" value="OK"/>
Number of observations per subgroup:	<input type="text" value="4"/>	<input type="button" value="OK"/>
Total number of observations:		<input type="text" value="40"/>

Figure 4.13: Preliminary sampling plan created by the PSMIS for the MSFC project.

After this is done, the analyst can proceed to create the actual sampling plan which would consist of the remaining 90 subgroups. The preliminary and actual subgroups are then merged by the PSMIS in order to obtain the total number of samples and to display the complete Pareto diagram and control charts (refer to Sections 3.6.3 and 3.6.4 for a complete explanation).

Exactly the same method employed in the MSFC project to establish the division of subgroups was utilized in the hoisting operation (KSC) case study: a random timer connected to a time lapse VCR (GYR, Model Number TLC3168HD). In this situation, the videotaped operations were split into 18 subgroups with 4 observations each. The preliminary sampling plan was composed of 4 samples, which resulted in 16 observations as depicted in Figure 4.14.

Set Preliminary Sampling Plan	
Number of groups:	<input type="text" value="1"/>
Number of subgroups per group:	<input type="text" value="4"/>
Number of observations per subgroup:	<input type="text" value="4"/>
<hr/>	
Total number of observations:	16

Figure 4.14: Preliminary sampling plan created by the PSMIS for the KSC project.

4.6 Statistical Significance

In order for a safety study to have statistical validity, the calculation of the number of observations needed, n' (n prime), to attain statistical significance is obligatory, where n' is determined from the data of the preliminary inspections. For the MSFC project, an L' of 10 %, a confidence level (CL) of 90 %, thus an $\alpha' = 0.10$ (10 % error), were considered to be appropriate by the analyst. Thus, the computation of \hat{p} , the percent of dendritics present in the preliminary study, is first necessary to determine the minimal sample size required (n') to obtain statistical reliability.

In the MSFC process, a total of 21 dendritics were recognized, which constituted the dendritic list. Additionally, there were 21 dendritic occurrences in the 40 random observations of the preliminary sampling study of the videotaped promoted combustion chamber testing operations (see Section 4.5), thus substituting into Equation 3.2 yields:

$$\hat{p} = \frac{\text{Number of dendritics observed in preliminary sampling}}{(\text{Total possible dendritics per observation}) * (\text{Number of observations})} = \frac{21}{21 * 40} = 0.025$$

To determine whether statistical significance was achieved, the \hat{p} value is substituted into Equation 3.3 which yields:

$$n' = \frac{4(z'_{\alpha/2})^2 \hat{p}(1 - \hat{p})}{(L')^2} = \frac{4 * 1.645^2 * 0.025 * (1 - 0.025)}{0.1^2} = 26.38 \cong 27 \text{ observations}$$

This result is evidence that statistical significance was attained since the actual number of random inspections ($n = 40$) was greater than the number of observations needed ($n' = 27$). Once again, these typed equations and calculations are also a true copy of the original computations, both for the MSFC and KSC case studies. However, the actual error for this study was not calculated by the analyst. The PSMIS performs these calculations plus has the advantage of also computing the actual error solving for α in Equation 3.3 and substituting n for the actual number of samples taken thus far. Figure 4.15 shows the values of \hat{p} (shown as “p^”), n , n' , and the actual error (α), among others.

Statistical Significance

Project:

Length of Interval: % (L')

Confidence Level: % (CL)

Percent Error: % (Desired Alpha)

Parameters

Z:

p^: Z':

L:

alpha/2:

Current Observations: (n)

Observations Needed: (n')

Actual Error: (Actual Alpha)

Figure 4.15: Statistical significance screen for the MSFC project provided by the PSMIS.

Similarly, for the hoisting operation study at KSC, an L' of 10 %, a CL of 90 %, hence an α' of 10 %, were deemed appropriate by the analyst as well. In addition, 57 dendritic elements composed the dendritic roster. Further, 12 dendritic occurrences were observed in the 16 inspections comprised in the preliminary sampling data set of the videotaped operations (view Section 4.5). Replacing into Equation 3.2 gives:

$$\hat{p} = \frac{\text{Number of dendritics observed in preliminary sampling}}{(\text{Total possible dendritics per observation}) * (\text{Number of observations})} = \frac{12}{57 * 16} = 0.013$$

According to Equation 3.3, the number of observations needed to attain statistical significance (n'), as calculated by the analysts of the KSC project, is the following:

$$n' = \frac{4z_{\alpha/2}^2 \hat{p}(1 - \hat{p})}{(L')^2} = \frac{4 * 1.645^2 * 0.013 * (1 - 0.013)}{0.1^2} = 14.05 \approx 15 \text{ observations}$$

In this safety study, the analyst did not calculate the actual error either. Figure 4.16 depicts the \hat{p} (shown as “p^”), n , n' , and the actual error (α) values, among others.

Statistical Significance

Project: Senior

Length of Interval: % (L')

Confidence Level: % (CL)

Percent Error: % (Desired Alpha)

Parameters

Z:

p^: Z':

L:

alpha/2:

Current Observations: (n)

Observations Needed: (n')

Actual Error: % (Actual Alpha)

Figure 4.16: Statistical significance screen for the KSC project provided by the PSMIS.

The PSMIS rounds up to the next integer the number of inspections needed for statistical significance. This is done since there cannot be a decimal or fraction of an observation.

4.7 Establish Control Limits and Control Charts

Several control chart procedures were introduced in Chapter 3 (Section 3.7). It is up to the system analyst to determine which control chart would be most advantageous to use. This decision can depend on the system being analyzed, data observed, availability of resources, time, system limitations, desired protection from unacceptable risks or hazards, desired results, *etc.*

Once the minimum amount of inspections to possess statistical impact (n') has been taken, the evaluator can choose to establish the control limits. Nevertheless, if n' has not been reached, the analyst can still decide to set up the control boundaries if he or she is satisfied with the actual error percentage, which is provided by the CHTFPM MIS (see Section 3.6.2.2 for a detailed description).

The first step in developing the control limits is the choice of a Shewhart or attribute chart, hence an applicable probability distribution. In the research of the promoted combustion testing operations, the application of the Poisson distribution was judged to be a good fit for the process. Therefore, the control charts that have an underlying Poisson distribution are the c and u chart.

As applied to this case study, the c chart was believed to be more suitable to represent the safety status of the promoted combustion testing system. The c chart will plot the total number of occurring dendritics (defects/nonconformities) per subgroup. In

other words, the dendritics within the 4 observations of each subgroup are summed, and that value is plotted. As stated before, the preliminary samples consisted of the first 10 subgroups where 21 dendritics occurred. The c chart parameters were generated by inputting the data of the preliminary study in Equations 3.4 through 3.6, as follows:

$$\text{Center Line} = \bar{c} = \frac{\sum_{i=1}^m c_i}{m} = \frac{21}{10} = 2.1 \quad (3.4)$$

$$UCL = \bar{c} + 3\sqrt{\bar{c}} = 2.1 + 3\sqrt{2.1} = 6.447 \quad (3.5)$$

$$LCL = \bar{c} - 3\sqrt{\bar{c}} = 2.1 - 3\sqrt{2.1} = -2.247 \therefore = 0 \quad (3.6)$$

Here, n is the total number of subgroups (10 samples of size 4). The collected data, or the number of dendritic occurrences, is positive in nature. Therefore, in the event of a negative LCL computation, a value of 0 (zero) is assigned.

It should be noted that \bar{c} is the process mean or center line which serves to find out the control limits: UCL and LCL. The control limits calculated by preliminary samples should be regarded as “trial” control limits, and the preliminary samples should be examined for lack of control. If there are no out-of-control conditions, then the “trial” limits can be adopted for future use.

That is why the CHTFPM MIS displays the graph of the preliminary sampling study, so the user can view if the system or process is stable. Once the end-user verifies that the system is in control, the assessor can utilize those control limits for the upcoming or future samples. If there are points outside the limits, the cause(s) for such outcome(s) should be investigated and addressed (please review Section 3.8 for dealing with out-of-control points). The fashion in which the PSMIS depicts the values of the control limits is

by clicking on the “See control limits” button (see Figures 4.15 and 4.16). Then a small screen appears where the analyst has to select the Shewhart chart of its preference in order to view the respective control limits, as illustrated in Figure 4.17. The c chart for the MSFC industrial scenario, constructed from the preliminary data set, is depicted in Figure 4.18 showing the values of the control parameters—center line, UCL and LCL.

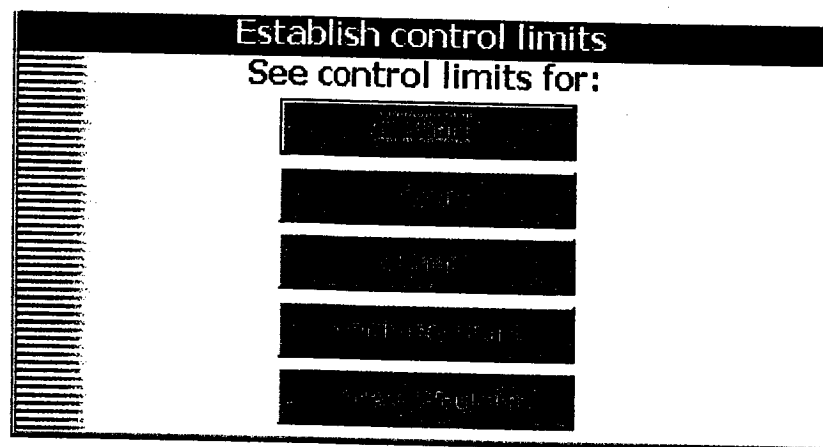


Figure 4.17: Screen for selecting the type of Shewhart chart control limits.

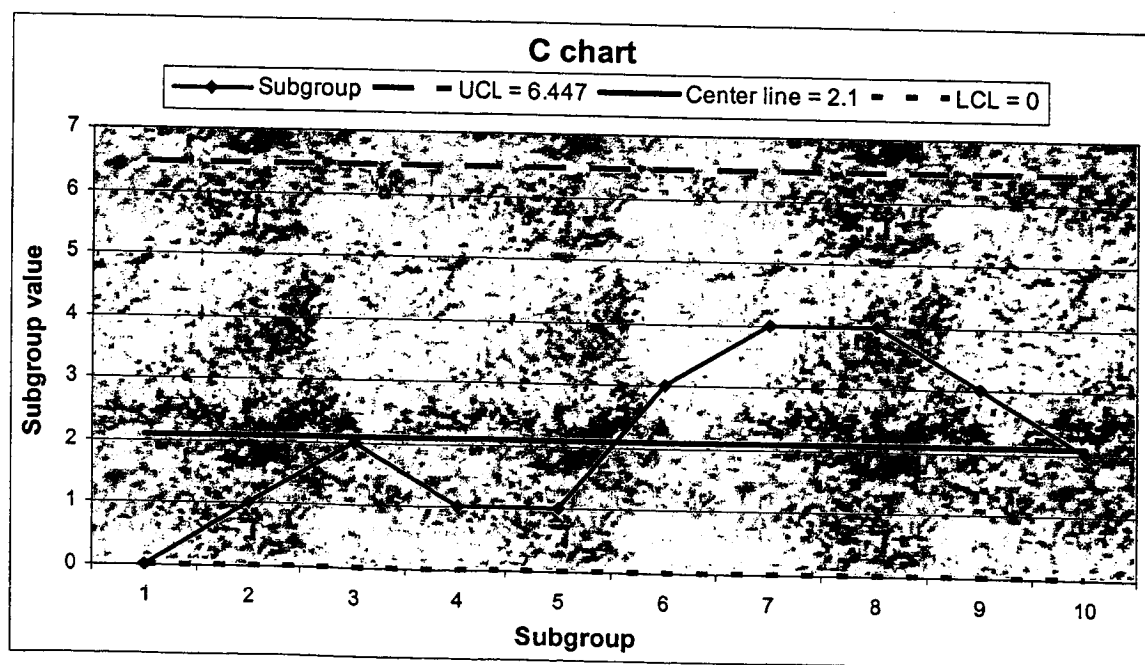


Figure 4.18: Control parameters of the c chart for the MSFC case study.

Likewise, the second predictive safety project also employed a Poisson distribution since it was considered to be suitable for the hoisting operation and testing of the HPGTs. In addition, a c chart was selected as well to provide assistance in depicting the safety status and stability of the process. In this case, 12 dendritics were observed in the first 16 inspections (4 subgroups of size 4) comprised in the preliminary samples. The c chart control limits were established by entering the information of the preliminary sampling in Equations 3.4 through 3.6 in the following manner:

$$\text{Center Line} = \bar{c} = \frac{\sum_{i=1}^m c_i}{m} = \frac{12}{4} = 3 \quad (3.4)$$

$$UCL = \bar{c} + 3\sqrt{\bar{c}} = 3 + 3\sqrt{3} = 8.196 \quad (3.5)$$

$$LCL = \bar{c} - 3\sqrt{\bar{c}} = 3 - 3\sqrt{3} = -2.2 \therefore = 0 \quad (3.6)$$

where n is the total number of subgroups (4 samples with 4 observations each).

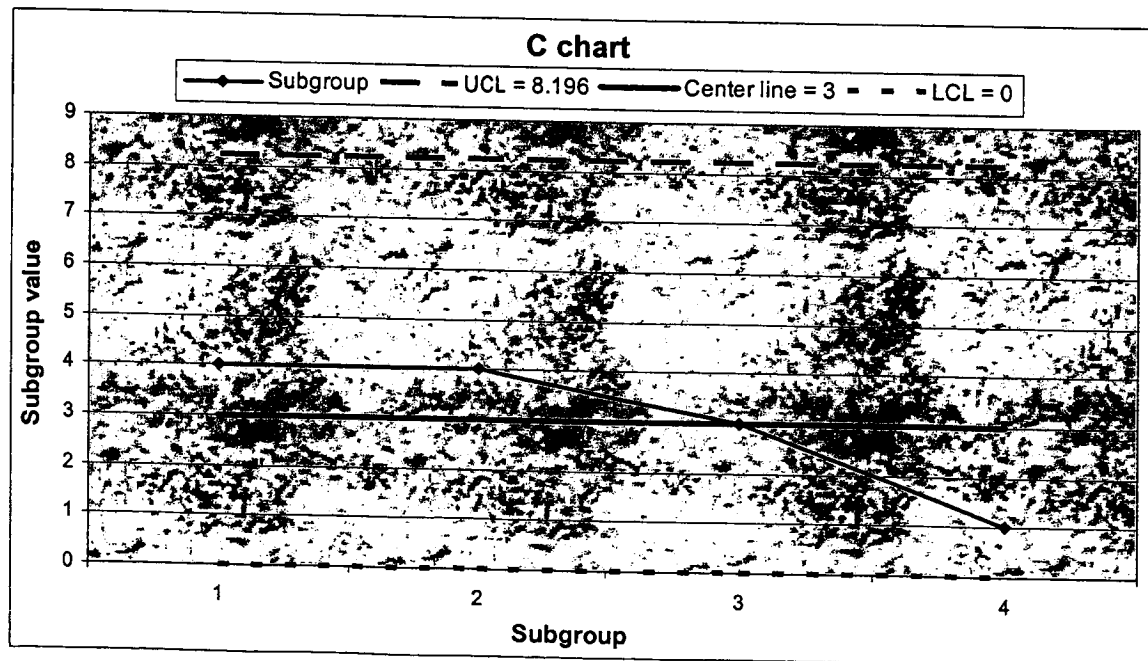


Figure 4.19: Control parameters of the c chart for the KSC case study.

Since there cannot be negative dendritics, there cannot be negative control limits either. The LCL in this occasion turned out to be a negative number; therefore, the correct lower control limit should be 0 (zero). For this case study, the pattern to obtain the control limits of the c chart, which are portrayed in Figure 4.19, was the same as the one followed in the MSFC project. This also means that the plotted values of every sample were obtained by adding the dendritic incidences in each subgroup.

4.7.1 Control Charts for the MSFC Case Study

As revealed before, a c chart was employed in the MSFC study to represent the safety status of the system under investigation. Figure 4.20 shows the c chart of this project, as constructed by the analyst. The values for the entire 100 samples or subgroups obtained from the MSFC project collected data are summarized in Appendix D.

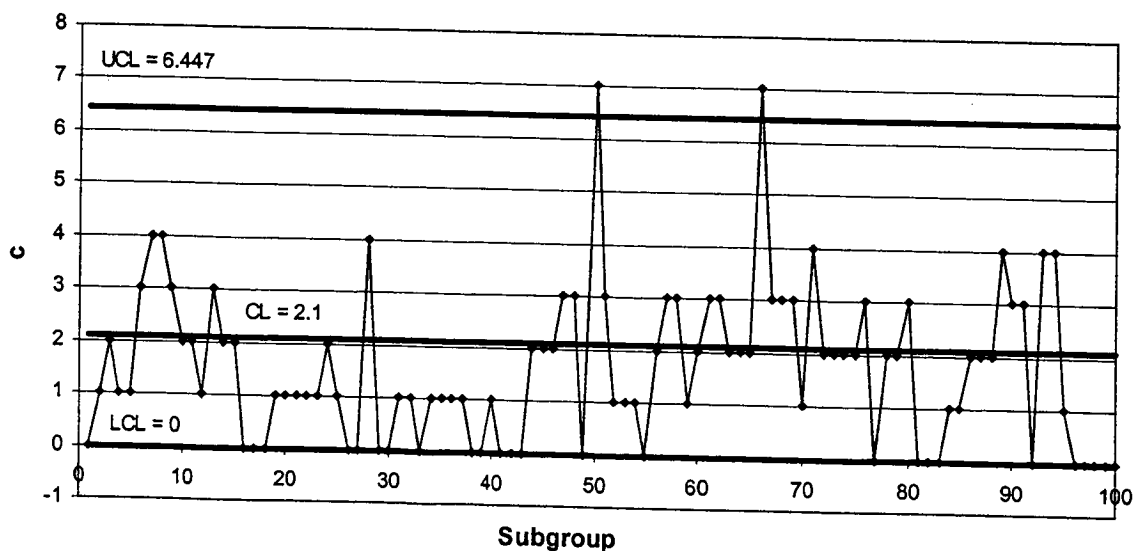


Figure 4.20: MSFC project c chart, as constructed by the analyst.

The CHTFPM MIS constructed the same c chart for the complete set of samples by just clicking a button. Figure 4.21 illustrates the c chart developed by the PSMIS.

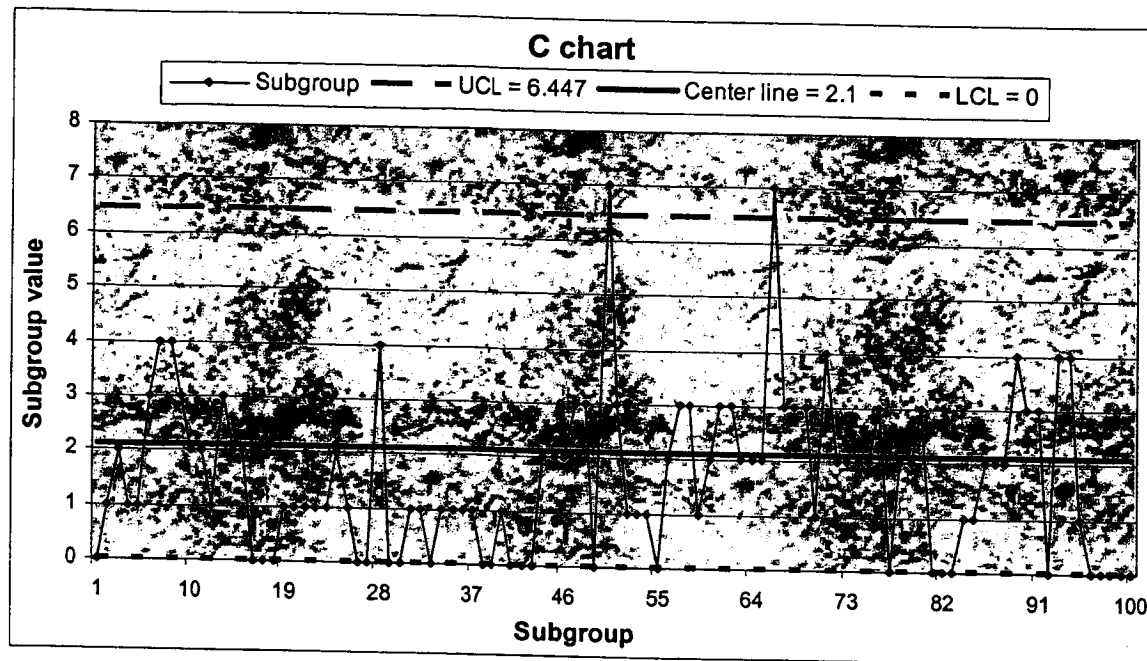


Figure 4.21: MSFC project c chart, developed by the PSMIS.

The distinctions between the two preceding figures are minor. For instance, the PSMIS chart starts the subgroup count with the number 1 (one) in the x axis, whereas the chart built manually includes the number 0 (zero) in the horizontal axis. It makes more sense to start the sample count at 1 since there is no subgroup number 0 (zero). In addition, the style of the control limits in the PSMIS chart are represented by dotted lines and their values are displayed along the legend keys, which are located at the top of the figure.

Additionally, a Pareto diagram can be formulated by the CHTFPM code at any moment during the safety study. This can provide an indication about which one of the dendritics has the highest frequency of occurrence. Therefore, a more focused attention can be better directed to correct those unsafe conditions. The Pareto analysis for this case

study is depicted in Figure 4.22, which was done by the analyst. The dendritics that did not occur during the data collection were not included in the Pareto diagram.

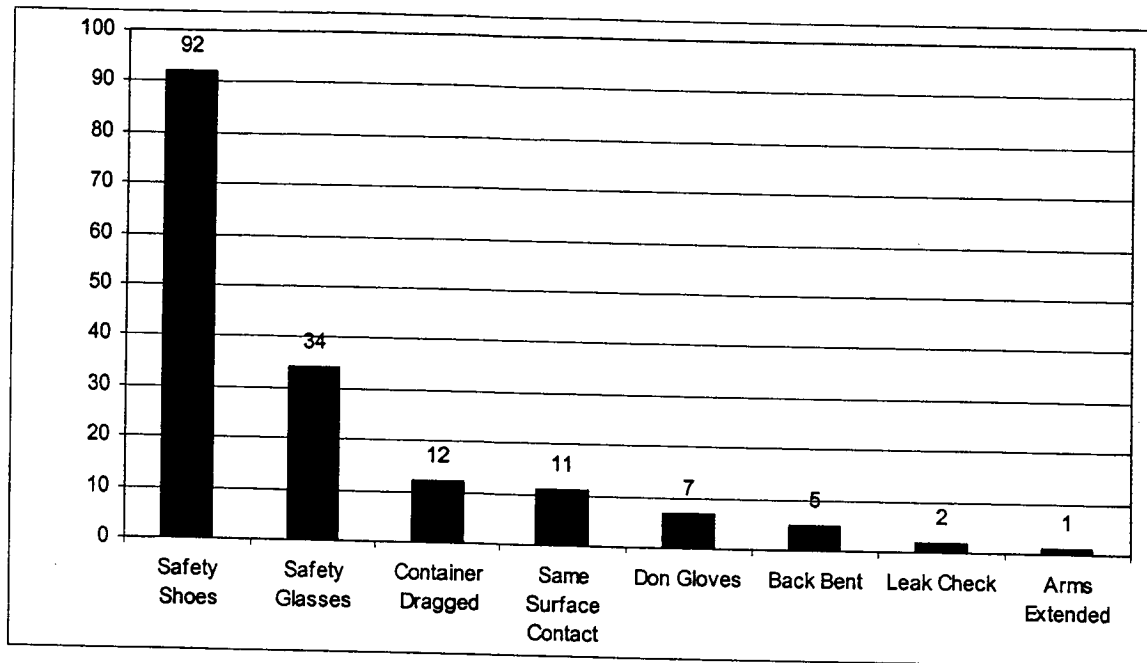


Figure 4.22: MSFC project Pareto diagram, as constructed by the analyst.

The Pareto diagram is created by the CHTFPM software program when the user specifies that action; Figure 4.23 depicts the Pareto plot, as developed by the CHTFPM MIS. Again, there are few dissimilarities between the manually-constructed and the PSMIS-developed Pareto diagram like background or bar colors, among others. For example, the description of each dendritic is abbreviated or rephrased in the original diagram, while the PSMIS copies the exact dendritic name from the dendritic list. One similarity, nonetheless, that both Pareto graphs have is that they do not include the dendritics that had a frequency or occurrence of 0 (zero).

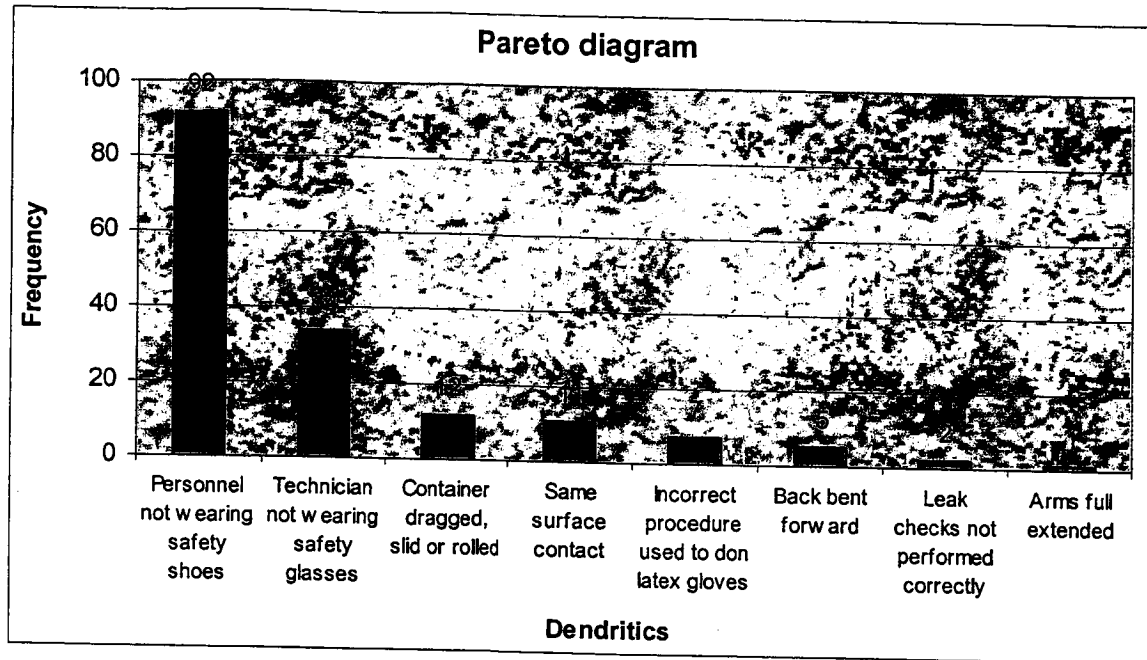


Figure 4.23: MSFC project Pareto diagram, developed by the PSMIS.

As described in Chapters 2 and 3, not all dendritics are equally impacting the safety of the system. In situations like this, what is needed is a method to classify dendritics according to severity, thus weighting the various types of dendritics in a reasonable manner. The method used to weight the dendritics or to assigned demerits to them is explained in Sections 2.4 and 3.5. As a result, the dendritics were split into four classes. Therefore, the dendritics that could cause more serious damage, either to the system or to the individuals, were clustered in the highest hierarchical category, which is Class A in this case. The dendritics in the second level of severity were lumped in Class B, and so forth. The results of this classification, which correspond to the MSFC case study, are shown in Table 4.1.

Table 4.1: Classification of dendritics for the MSFC project.

Class A Dendritic	Class B Dendritic	Class C Dendritic	Class D Dendritic
Failure to adhere to Standard Operating Procedure (SOP)	Incorrect procedure used to don latex gloves	Leak checks not performed after hookup or not performed correctly	Full and empty oxygen containers stored together
Back bent forward while lifting object	Same surface contact (bare hand and latex glove)	Personnel not wearing safety shoes in test area	Test cell used for storage
Arms full extended to the front while lifting	Personnel wearing dirty latex gloves	Oxygen container(s) not secured during combustion testing	Personnel limitations for test cell exceeded
Technician not wearing safety glasses when connecting/disconnecting oxygen bottles		Container(s) moved without using hand truck	Valve cap not installed when oxygen container(s) in use
		Container(s) not secured during movement	Oxygen container(s) not stored in upright position
		Test area not in "limited access control"	Trash and combustibles in test area
		Oxygen container dragged, slid or rolled	Oxygen container lifted by valve cap

The CHTFPM MIS categorizes the dendritics into the corresponding groups according to the weights that the user assigned to them when creating the dendritic list as seen in Figures 4.7 (b) and 4.8 (b). In other words, the dendritics with the same highest weight are grouped in class A; the dendritics with the second highest weight are grouped into class B, and so on. Even though the PSMIS default weight values are 100, 50, 10 and 1 for the dendritics of Class A, B, C and D, respectively, a different set of weights reasonable for a specific problem may also be used. Moreover, it should be noted that the user can change these weights at any time.

The parameters for the weighted chart are calculated in the following equations (Equations 3.17 through 3.20), and the data used in such calculations is summarized in Appendix E. Figure 4.24 portrays the weighted chart with its control limits, as constructed

by the system evaluator.

$$\text{Center Line} = \bar{u} = 100\bar{u}_A + 50\bar{u}_B + 10\bar{u}_C + \bar{u}_D \quad (3.17)$$

$$\text{Center Line} = \bar{u} = 100(0.1) + 50(0.1) + 10(0.325) + 0 = 18.25$$

$$\hat{\sigma}_u = \left[(100)^2 \bar{u}_A + (50)^2 \bar{u}_B + (10)^2 \bar{u}_C + \bar{u}_D \right]^{1/2} \quad (3.20)$$

$$\hat{\sigma}_u = \left[(100)^2 (0.1) + (50)^2 (0.1) + (10)^2 (0.325) + 0 \right]^{1/2} = 35.812$$

$$UCL = \bar{u} + 3\hat{\sigma}_u = 18.25 + 3(35.812) = 125.686 \quad (3.18)$$

$$LCL = \bar{u} - 3\hat{\sigma}_u = 18.25 - 3(35.812) = -89.186 \therefore = 0 \quad (3.19)$$

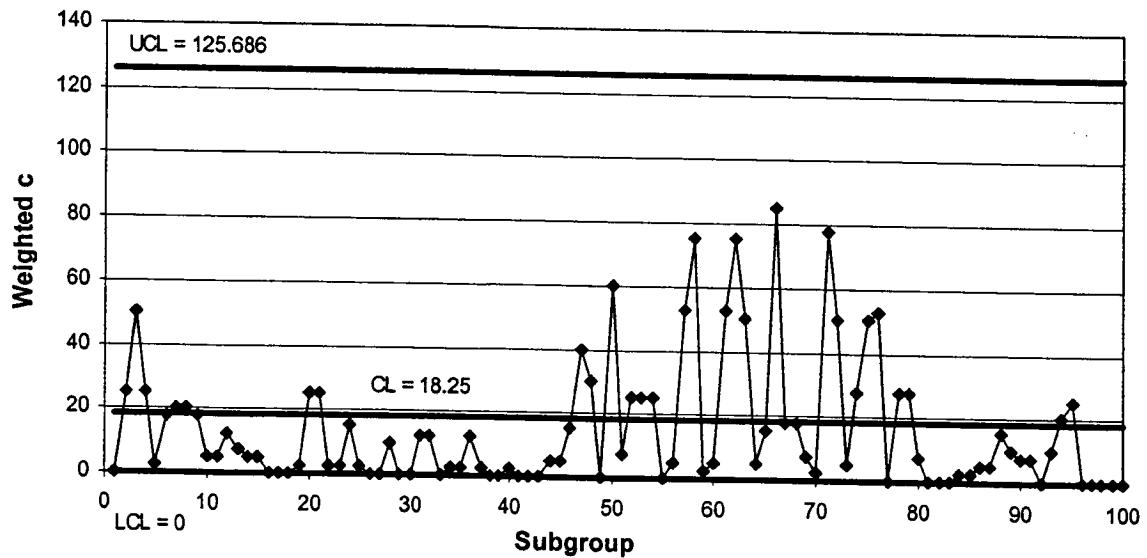


Figure 4.24: MSFC project weighted chart, as constructed by the analyst.

The PSMIS performs all of the previous computations automatically to find out the control limits for the weighted chart and depicts their values on the graph, as observed in Figure 4.25. Additionally, all the control charts produced by the CHTFPM MIS are consistent in their format.

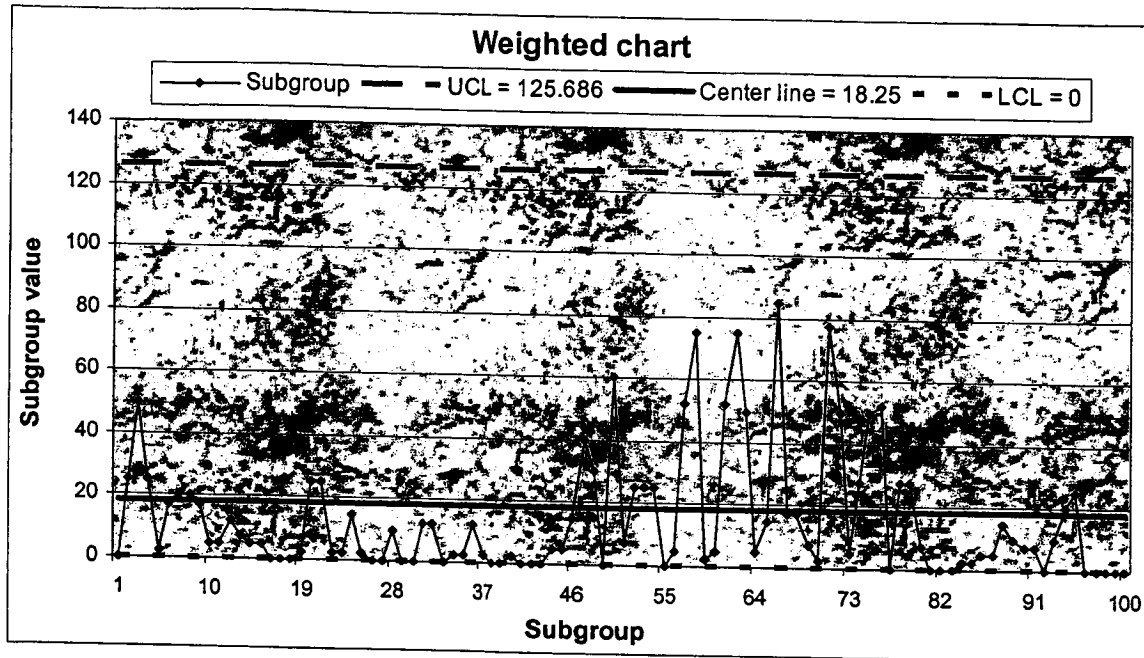


Figure 4.25: MSFC project weighted chart, developed by the PSMIS.

As mentioned previously in Section 3.7.5, the EWMA control chart is a good alternative to the Shewhart control chart when small shifts in the safety mean, in the order of 1.5σ or less, need to be detected. The first step in setting up an EWMA control chart is determining the parameters L and λ . Using Table 3.2 in Chapter 3, the elected parameters L and λ were 3.054 and 0.4, respectively. These values were chosen to detect a shift in the safety mean of 1.00 with an ARL_0 of 500 and the ARL_1 for an out of control system of 14.3 (it will take at least 15 samples to detect the shift with a point outside of the control limits).

The center line for the EWMA chart is also the same as the one from the selected Shewhart chart, which is the c chart in this case. Utilizing Equations 3.23 up to 3.26, the plotted points and control boundaries were obtained, respectively. The resulting EWMA control chart, as constructed by the analyst, is represented in Figure 4.26 (Appendix F

encapsulates the data used to construct this chart), while Figure 4.27 shows the EWMA generated by the PSMIS.

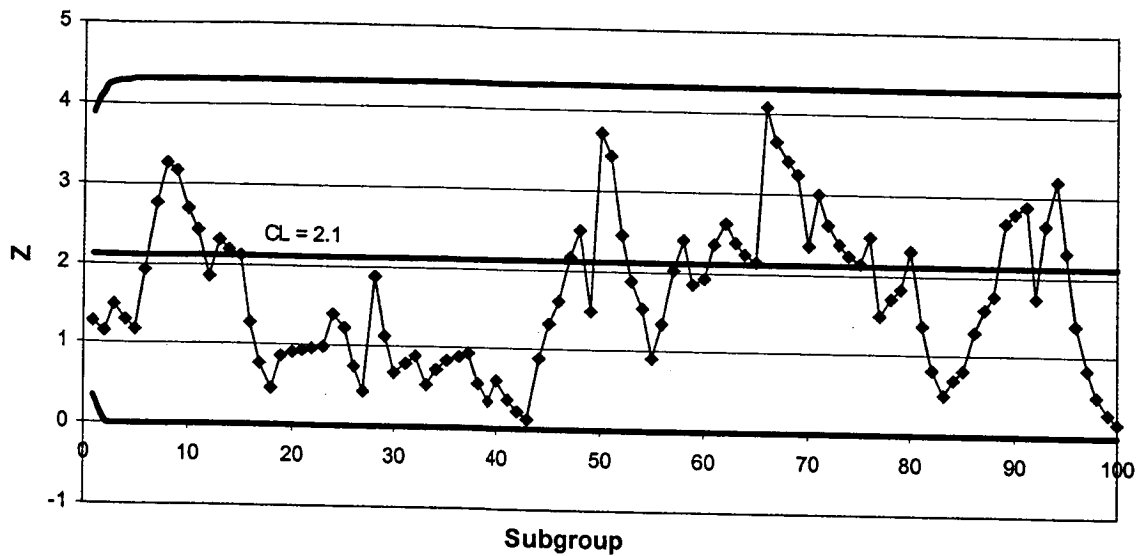


Figure 4.26: MSFC project EWMA chart ($L = 3.054$ and $\lambda = 0.4$), as constructed by the analyst.

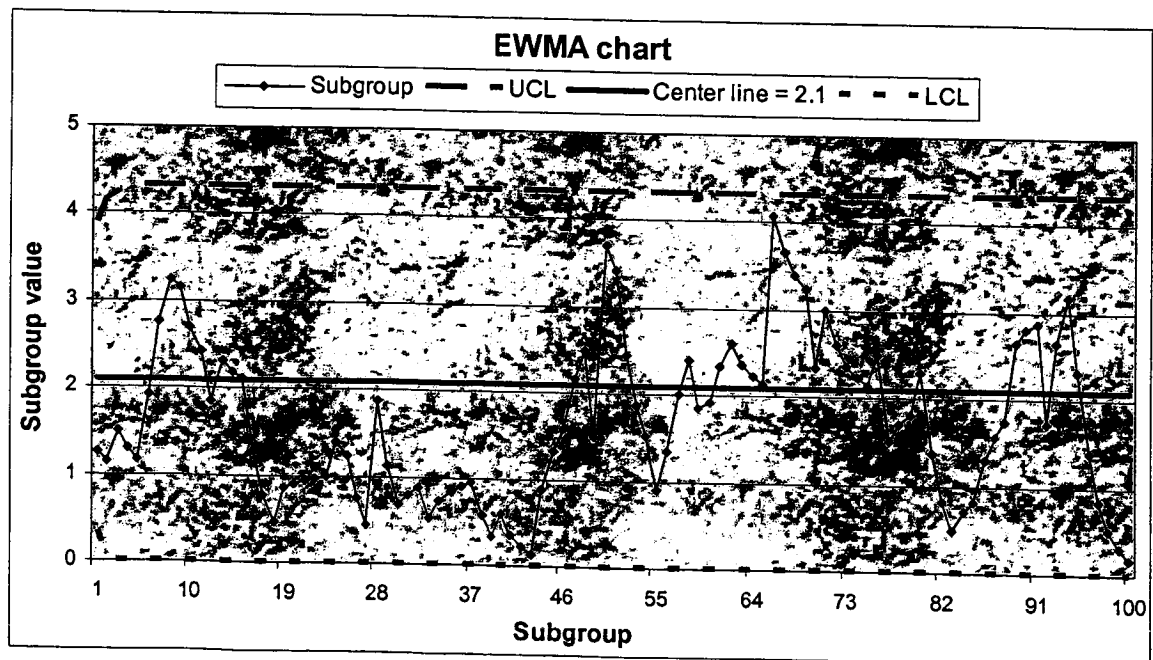


Figure 4.27: MSFC project EWMA chart ($L = 3.054$ and $\lambda = 0.4$), developed by the PSMIS.

In both EWMA charts, the control limits are not shown for the reason that they are not constant; that is, each sample has its own set of control limits. However, the control limits, both the UCL and LCL, tend to reach steady-state as the subgroup number increases.

In addition, a second EWMA control chart was plotted to demonstrate the different levels of sensitivity that can be attained using this control chart. Suppose the same ARL_0 and shift in the safety mean as above are desired but the shift in the safety mean needs to be detected quicker, say in 10 samples. Using Table 3.2 from Chapter 3, the values for the parameters λ and L were 0.10 and 2.814, accordingly. Equations 3.23 through 3.26 equations were also used to construct this EWMA chart along with the data provided in Appendix G. Figure 4.28 portrays the resultant EWMA chart, as created by the analyst.

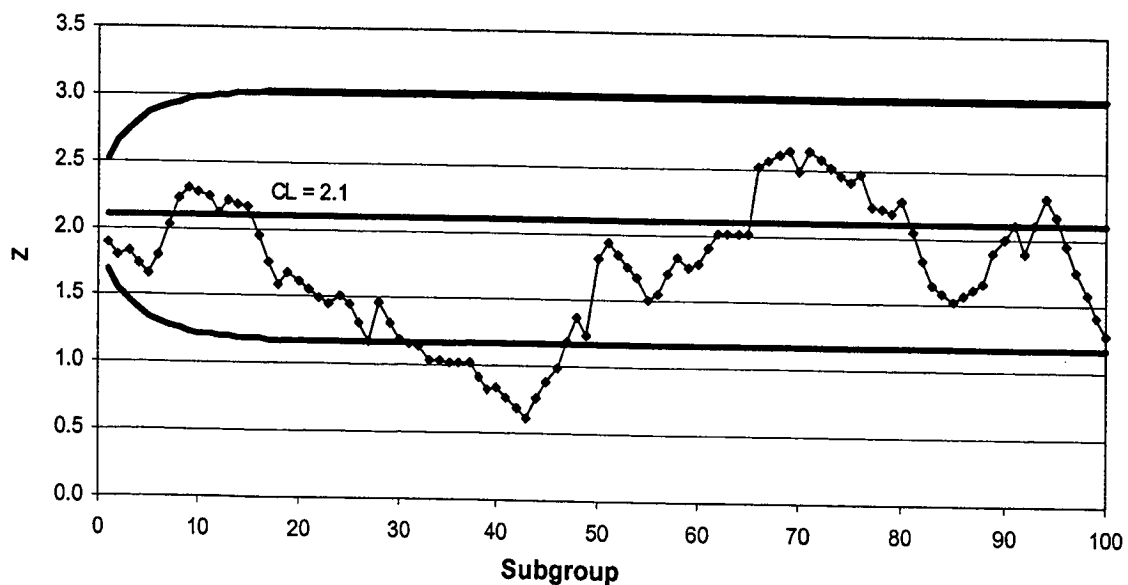


Figure 4.28: MSFC project EWMA chart ($L = 2.814$ and $\lambda = 0.1$), as constructed by the analyst.

The associated pair of the second EWMA control chart, which was developed using the PSMIS, is shown in Figure 4.29 below.

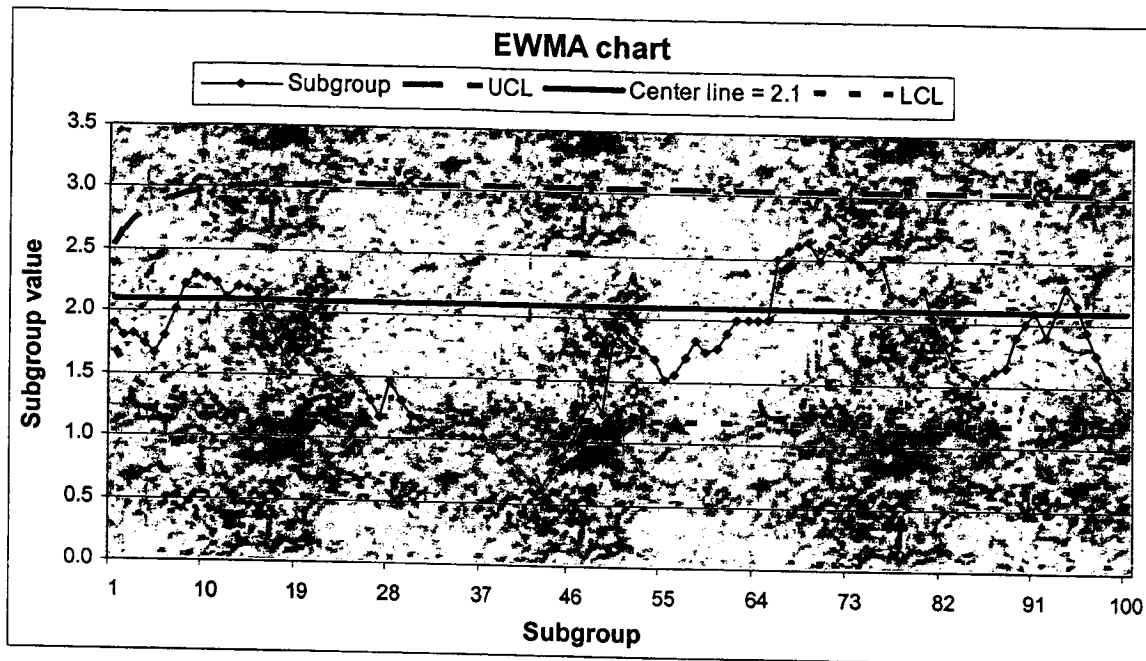


Figure 4.29: MSFC project EWMA chart ($L = 2.814$ and $\lambda = 0.1$), developed by the PSMIS.

A good way to further improve the sensitivity of the control procedure to large shifts without sacrificing the ability to detect small shifts quickly is to combine a Shewhart and EWMA chart. These combined control procedures are effective against both large and small shifts. For example, plotting Figures 4.20 and 4.28 on the same graph gives the combined Shewhart-EWMA control chart, which is illustrated in Figure 4.30. It should be recalled that the analyst had to do this combination manually (by manipulating the data) as all the other control charts and calculations shown earlier in this chapter. On the other hand, the PSMIS performed this combination automatically; Figure 4.31 displays the combined Shewhart-EWMA chart given by the PSMIS.

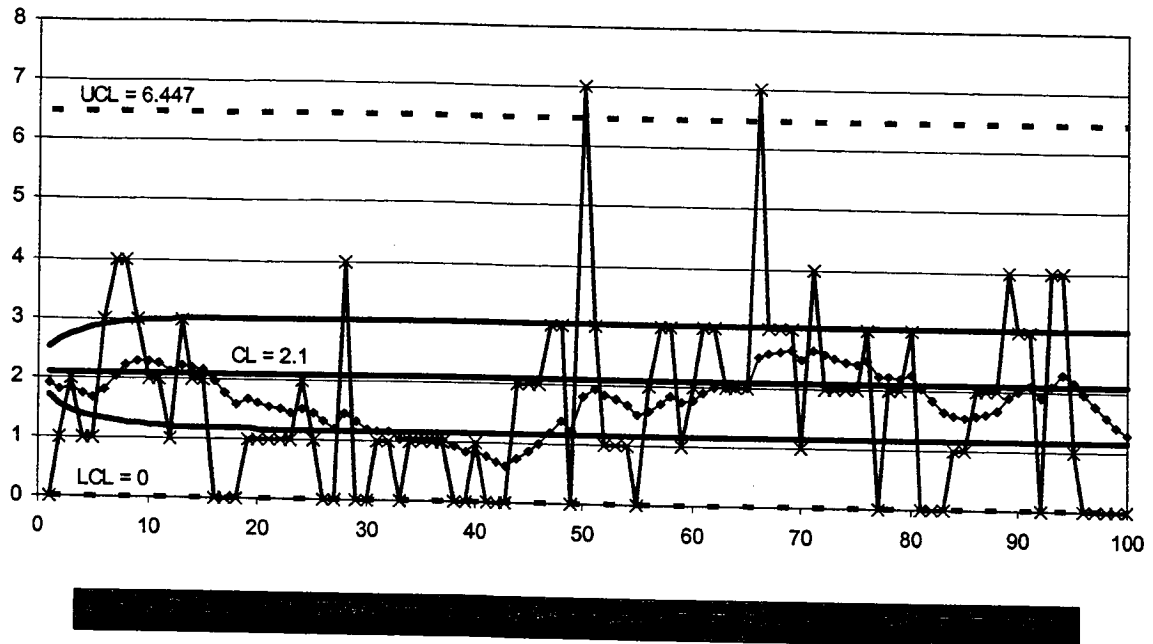


Figure 4.30: MSFC project combined Shewhart-EWMA chart ($L = 2.814$ and $\lambda = 0.1$), as constructed by the analyst.

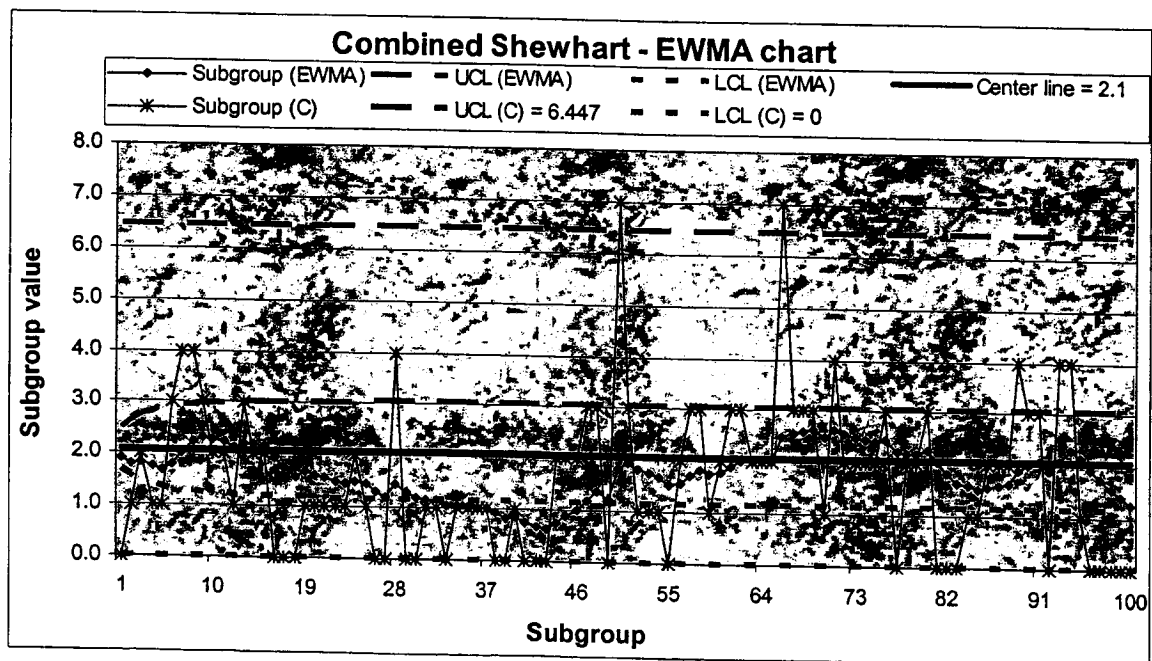


Figure 4.31: MSFC project combined Shewhart-EWMA chart ($L = 2.814$ and $\lambda = 0.1$), developed by the PSMIS.

4.7.2 Control Charts for the KSC Case Study

The KSC case study also used a c chart as the basis for predictive safety; therefore, the same procedure pertaining to the MSFC project was followed in order to obtain the results sought. Nonetheless, it is important to point out that for the testing, preparation and hoisting operation of the HPGETs the analyst just created two control charts, the c chart and the weighted chart, as well as the Pareto diagram. Consequently, these two charts were the only ones developed by the CHTFPM MIS in conjunction with the Pareto plot. The data used to build the c chart for the KSC study is enclosed in Appendix L, and the complete c chart elaborated by the analyst is depicted in Figure 4.32.

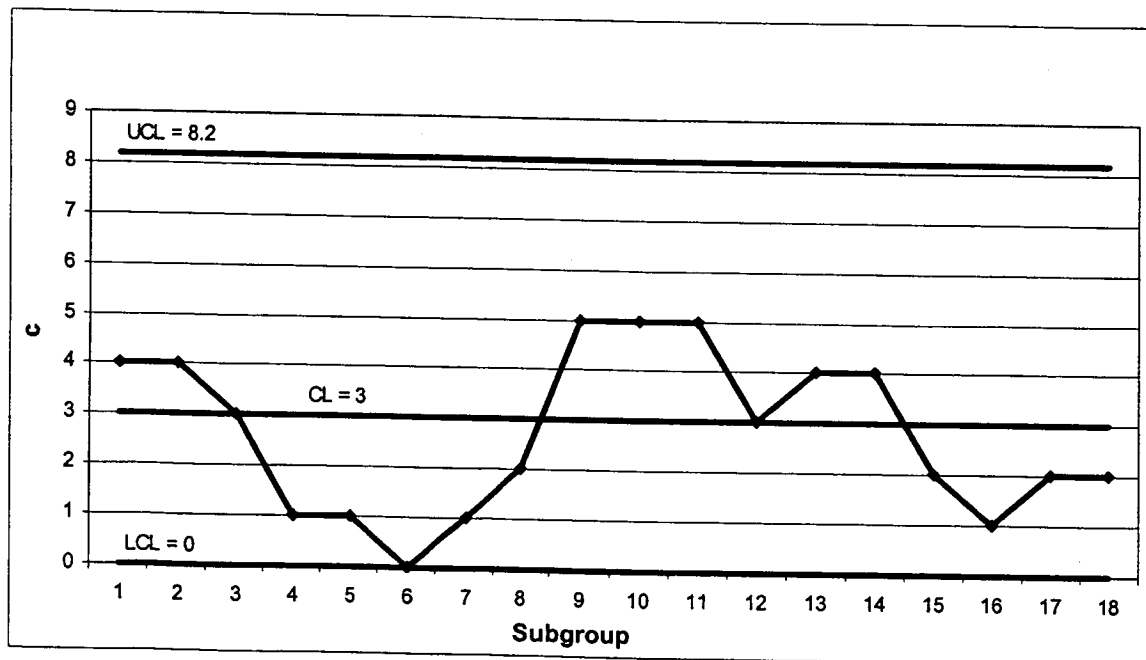


Figure 4.32: KSC project c chart, as constructed by the analyst.

The corresponding reproduction by the PSMIS of the above c control chart is portrayed in Figure 4.33.

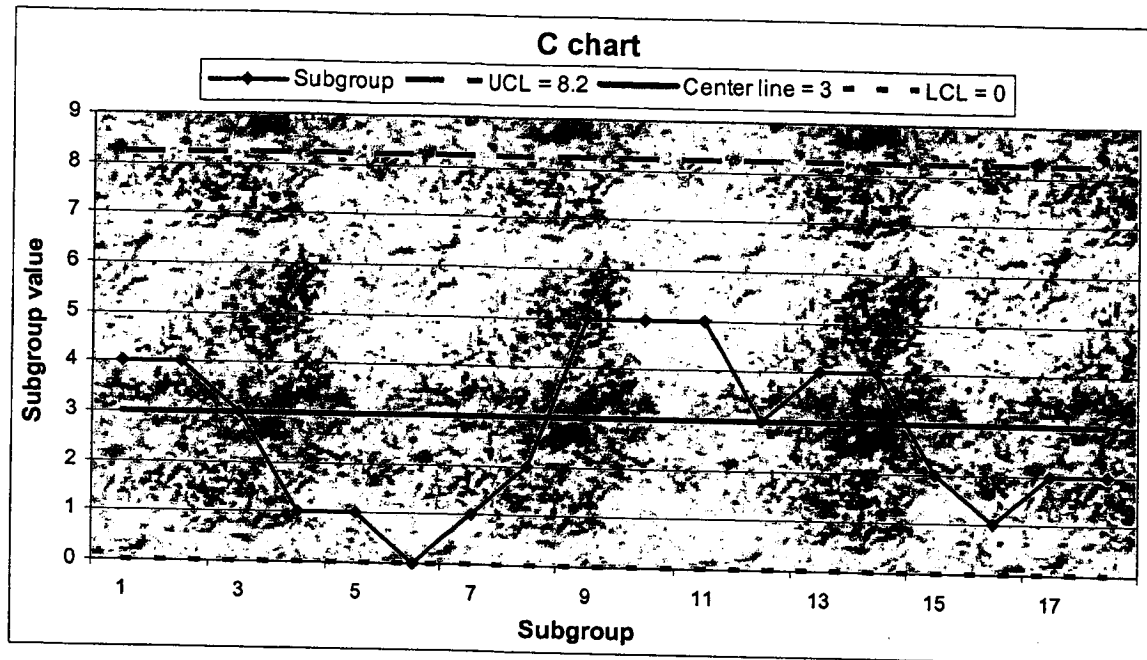


Figure 4.33: KSC project c chart, developed by the PSMIS.

A Pareto diagram was also built for this case scenario by the analyst and is represented in Figure 4.34.

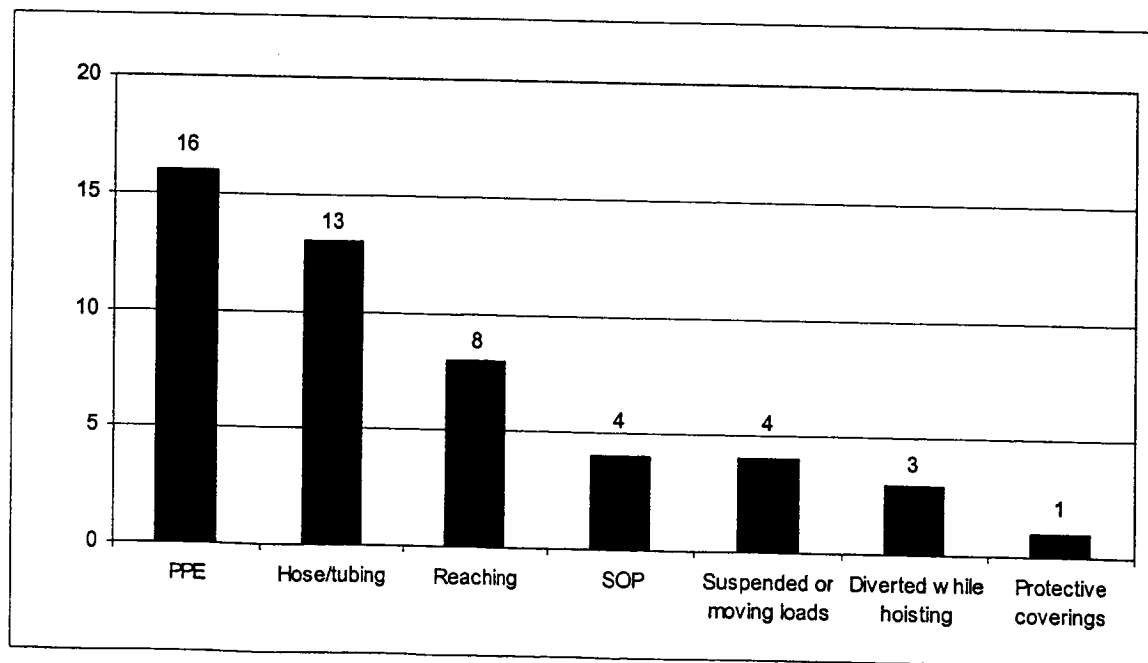


Figure 4.34: KSC project Pareto diagram, as constructed by the analyst.

Figure 4.35, as produced by the CHTFPM software package, displays the duplicate of the manual Pareto diagram,

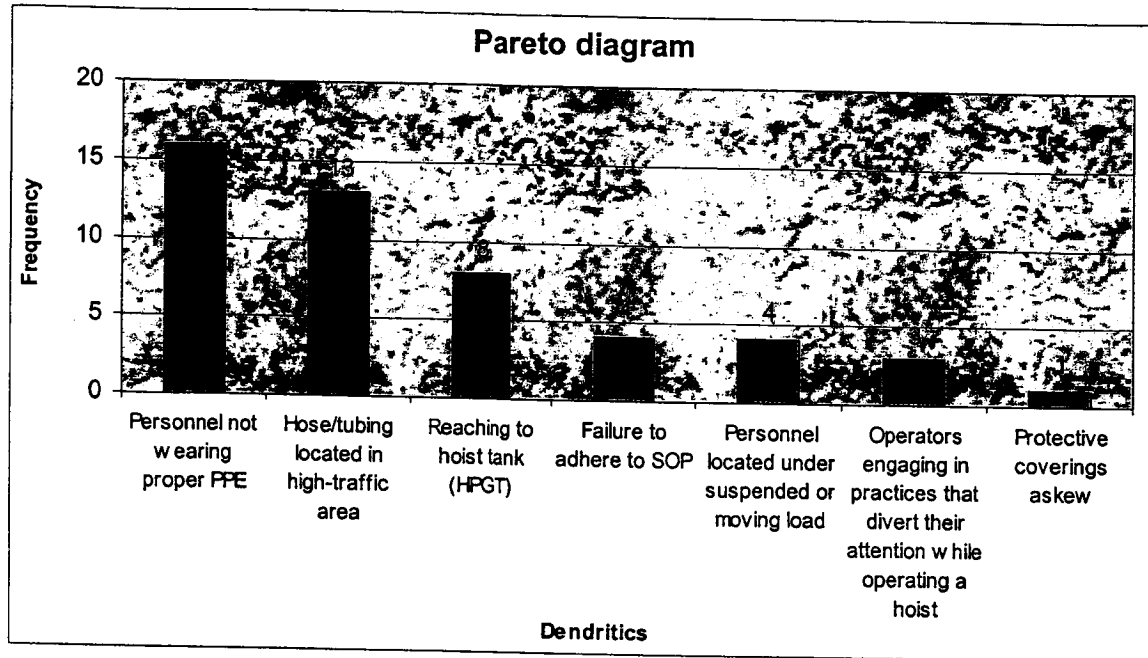


Figure 4.35: KSC project Pareto diagram, developed by the PSMIS.

Since not all the dendritic elements have the same weight or are equally severe, a weighted chart can provide a means of knowing if the process or system is becoming hazardous due to the committed dendritics. For this project, the pursued technique to categorize the dendritics into classes was the same as the one employed in the MSFC case study. This denotes that there were four dendritic categories in this case. Appendix K describes the arrangement of the dendritics into classes or groups for the KSC safety project. The equations used to calculate the parameters for the weighted chart pertaining to this project were also Equations 3.17 through 3.20.

$$\text{Center Line} = \bar{u} = 100\bar{u}_A + 50\bar{u}_B + 10\bar{u}_C + \bar{u}_D \quad (3.17)$$

$$\text{Center Line} = \bar{u} = 100(0.625) + 50(0) + 10(0.6875) + 0 = 13.125$$

$$\hat{\sigma}_u = \left[(100)^2 \bar{u}_A + (50)^2 \bar{u}_B + (10)^2 \bar{u}_C + \bar{u}_D \right]^{1/2} \quad (3.20)$$

$$\hat{\sigma}_u = \left[(100)^2 (0.625) + (50)^2 (0) + (10)^2 (0.6875) + 0 \right]^{1/2} = 26.339$$

$$UCL = \bar{u} + 3\hat{\sigma}_u = 13.125 + 3(26.339) = 92.142 \quad (3.18)$$

$$LCL = \bar{u} - 3\hat{\sigma}_u = 13.125 - 3(26.339) = -65.892 \therefore = 0 \quad (3.19)$$

Appendix M contains the data employed in the preceding computations and Figure 4.36 shows the weighted chart for the KSC industrial scenario, as formulated by the analyst.

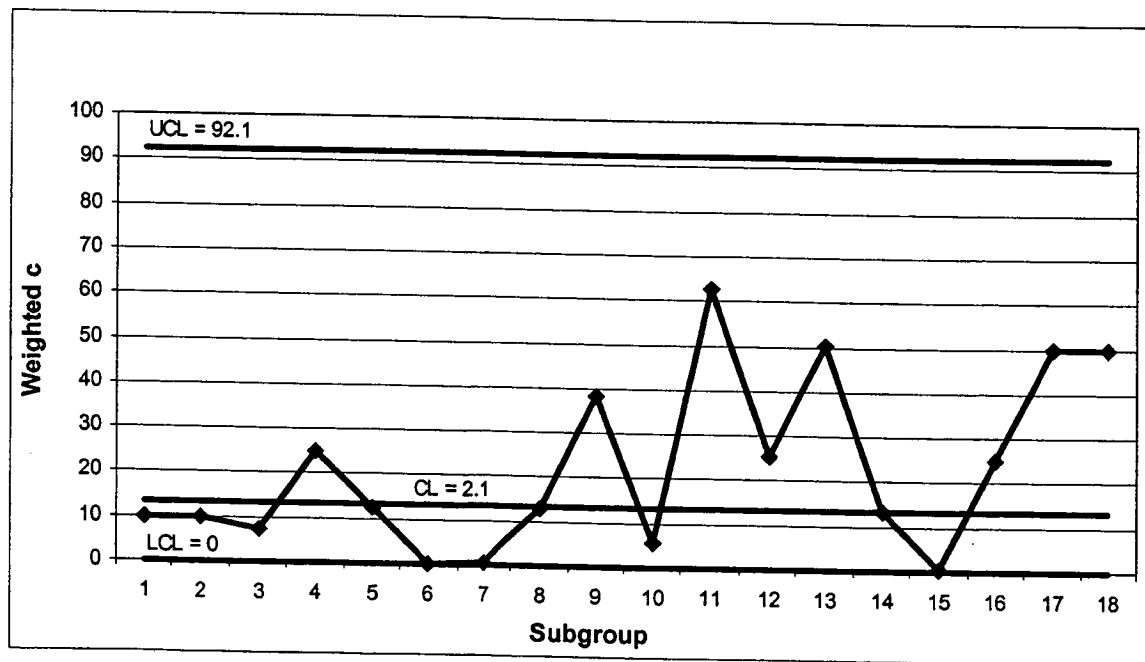


Figure 4.36: KSC project weighted chart, as constructed by the analyst.

The CHTFPM MIS performs the necessary calculations to determine the weighted chart control limits and displays their values on the figure next to the corresponding legend keys. Figure 4.37 illustrates the weighted chart as constructed by the PSMIS.

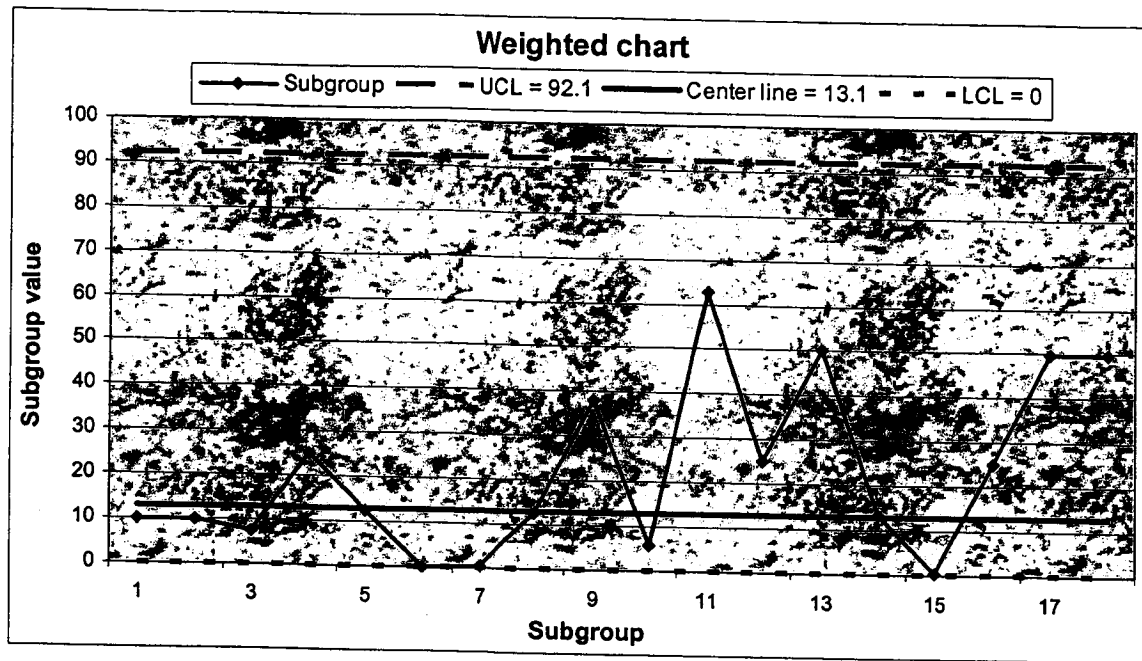


Figure 4.37: KSC project weighted chart, developed by the PSMIS.

As elucidated throughout this chapter, the control charts were made manually by the respective analysts by performing the necessary calculations and control charts in Microsoft Excel. However, they had to indicate to the software application what to do and how to do it. That is, they had to manipulate and handle the data themselves, instead of the program doing it for them, as is explained in the next section.

4.8 Reliability and Efficiency of the PSMIS

To determine the reliability of the computer program, the CHTFPM MIS had to be tested using the two previously described predictive safety studies, which had been validated; therefore, such results are correct. This comparison was done to show that the results calculated by hand were exactly the same as those obtained with the PSMIS. The

exhaustive and methodical evidence shown in Section 4.7 clearly confirms that the outcomes given by the CHTFPM software system are true and accurate, ensuing in a thorough reliability of the program.

As far as the effectiveness is concerned, the CHTFPM MIS was rated in terms of the time and manpower required to complete the two safety studies. In order to explain this subject, it is vital to understand how the projects under consideration were accomplished manually. First, the analysts of the two case scenarios had to create the forms of the PHA, FMEA and barrier analysis. This can be done in Microsoft Word or Excel. Second, after defining the dendritic list, they had to develop and print sampling sheets to conduct the observations at the site of investigation. This also can be achieved in Microsoft Word or Excel. Third, the sampling plan had to be formulated. This can be done in Microsoft Excel, which can generate random times, or by any other method; in both case studies, the random sampling plan was performed using the time lapse VCR and the random timer.

Fourth, the sampling sheets had to also be created in Excel in order to enter and count the number of dendritics observed. Then the necessary arithmetic operations to determine the subgroup values had to be input into the software application. This implies specifying which cells have to be added, multiplied, divided, *etc.* Furthermore, the equations for calculating the control chart parameters—center line, LCL, UCL, $\hat{\sigma}_u$, *etc.*—had to be input into the software application. After that, the analysts also had to manipulate the data and specify to the computer program which values to plot and how to plot them.

This manual process is time consuming and prone to error, especially at the time of entering the control chart equations. In addition, this type of analysis can take days or even weeks just to set up. After having an idea about the amount of work required to complete a project as the ones described in this chapter, it will be easier to understand the effectiveness or efficiency of the PSMIS.

The efficiency of the two case scenarios was determined by taking into account the factors of effort and time required to complete the project. The effort element or manpower is represented by the number of persons (NP) involved in the achievement of the investigation, and the time factor is represented by the average number of hours per person ($ANHPP$) spent to conclude the study. These two constituents provide the total number of hours (TNH) used up in the completion of the safety project which can be expressed as the following formula:

$$TNH = (ANHPP) (NP) \quad (4.1)$$

The efficiency (E) of the PSMIS is computed by Equation 4.2 below:

$$E = 1 - \left(\frac{TNH_{PSMIS}}{TNH_{Manually}} \right) \quad (4.2)$$

The formula expressed above implies that it is first obligatory to compute both the TNH_{PSMIS} and the $TNH_{Manually}$. The TNH_{PSMIS} corresponds to the hours it took to complete the project using the PSMIS. $TNH_{Manually}$ stands for the hours invested in the completion of the study when it was done manually or without the aid of the CHTFPM MIS. If the TNH_{PSMIS} is less than the $TNH_{Manually}$, then a positive efficiency exists.

In fact, the efficiency can be negative. For example, if the TNH_{PSMIS} is greater than the $TNH_{Manually}$, the ratio of these two values as illustrated in Equation 4.2 will be higher than 1 (one). This will ensue in a negative efficiency, which signifies that there is no improvement or advantage in using the PSMIS because it took more time to realize the whole analysis with the CHTFPM MIS than without it (manually).

The efficiency can also be 0 (zero) if both the TNH_{PSMIS} and the $TNH_{Manually}$ are the same. If this is the case, the ratio of these two components will give a value of 1 (one); therefore, in the efficiency equation the result will be: $1 - 1 = 0$. The rationale in this circumstance is that no benefit is gained or lost by using the CHTFPM MIS because it takes the same time to carry out the safety experiment with or without the use of the PSMIS.

4.8.1 Efficiency of the PSMIS in the MSFC Case Study

To complete the MSFC project, it took 3 persons who were working 10 hours per week for 3 months. The amount of time employed in watching the videotaped operations in order to perform the PHA, FMEA and barrier analysis was not included for the calculation of the efficiency. The reason for this is because that time would also have to be spent when using the PSMIS. Otherwise, it would not be possible to develop the three previous analyses, thus the dendritic list, since the analyst would not have sufficient knowledge about the system or process. Therefore, the hours that count as part of the study are those between the initial moment when the analyst started doing the PHA and when the final control chart was completed. Additionally, the time it took to collect the

data with the sampling sheets is not part of the number of hours necessary to conclude the study because this is also mandatory when utilizing the PSMIS.

Based on the justification previously presented, it was estimated that 2 weeks were consumed to gain valuable insight about the system or process of the promoted combustion testing operations. Therefore, those 2 weeks were not counted toward the efficiency. Assuming there are 4 weeks in each month, the total number of weeks in a period of 3 months is 12. However, due to the 2 weeks utilized in becoming familiar with the system in order to recognize any anomalies, the actual number of weeks that were spent to fulfill the project becomes 10. Multiplying the actual number of weeks times the number of worked hours in every week by an individual (10 hours) gives a total of 100 hours. This denotes that each person involved in this case study put in 100 hours of work during the course of three months. Consequently, the $ANHPP_{Manually}$ is computed as given below.

$$ANHPP_{Manually} = \frac{(100 + 100 + 100) \text{ hours}}{3 \text{ persons}} = \frac{100 \text{ hours}}{\text{person}}$$

So, replacing this average into Equation 4.1 gives the following:

$$TNH_{Manually} = (ANHPP_{Manually})(NP_{Manually}) = \left(\frac{100 \text{ hours}}{\text{person}} \right) (3 \text{ persons}) = 300 \text{ hours}$$

Likewise, the TNH_{PSMIS} can be found. When the PSMIS was utilized in the MSFC predictive safety study, it was done by 1 (one) individual who finished the project in 3 hours. So, the TNH_{PSMIS} is computed in the following fashion:

$$ANHPP_{PSMIS} = \frac{3 \text{ hours}}{1 \text{ person}} = \frac{3 \text{ hours}}{\text{person}}$$

$$TNH_{PSMIS} = (ANHPP_{PSMIS})(NP_{PSMIS}) = \left(\frac{3 \text{ hours}}{\text{person}} \right) (1 \text{ person}) = 3 \text{ hours}$$

Therefore, by substituting the $TNH_{Manually}$ and TNH_{PSMIS} values into Equation 4.2 yields:

$$E = 1 - \left(\frac{TNH_{PSMIS}}{TNH_{Manually}} \right) = 1 - \left(\frac{3 \text{ hours}}{300 \text{ hours}} \right) = 0.99 = 99 \%$$

Table 4.2 encapsulates the MSFC data of the time and manpower required to conclude the project manually versus with the PSMIS.

Table 4.2: Summary of the efficiency elements for the MSFC project.

Element	Manually	PSMIS
Avg. hours worked per person ($ANHPP$)	100	3
Persons involved in project (NP)	3	1
Total hours to complete project (TNH)	300	3
Efficiency of the PSMIS (E)	99 %	

4.8.2 Efficiency of the PSMIS in the KSC Case Study

For the KSC case study, 3 people participated in the project for 3 months, and each individual worked 10 hours per week. The same rationale explained for the MSFC industrial scenario in the previous section was also suitable and appropriate for the KSC operations. The only hours that were considered toward the efficiency computation were those spent in typing in all the project information into the PSMIS. Therefore, the time of watching the videotaped operations to perform the PHA, FMEA and barrier analysis and

the time to manually record the dendritic occurrences in the sampling sheets were not included in the calculations. Consequently, the time to become familiar with the process in order to identify potential hazards was estimated to be 2 weeks as well.

Additionally, the same assumption for the MSFC project, stating that each month has 4 weeks, was made in the KSC case study. Hence, the weeks encompassed in the 3-months duration of the project are 12, but because of the 2 weeks spent in becoming familiar with the process to recognize the dendritics, the actual number of weeks considered in the calculations is 10. The full amount of hours that each analyst worked is found by multiplying the actual number of weeks and the number of hours that he or she worked in every week (10 hours); this equals to a total of 100 hours. Since 3 persons contributed to the realization of the KSC project, the $ANHPP_{Manual}$ yields the following:

$$ANHPP_{Manually} = \frac{(100 + 100 + 100) \text{ hours}}{3 \text{ persons}} = \frac{100 \text{ hours}}{\text{person}}$$

By substituting this number into Equation 4.1, it results in:

$$TNH_{Manually} = (ANHPP_{Manually})(NP_{Manually}) = \left(\frac{100 \text{ hours}}{\text{persons}} \right) (3 \text{ persons}) = 300 \text{ hours}$$

Likewise, the TNH_{PSMIS} can be obtained. When the PSMIS was employed, the KSC safety study was completed in 4 hours by 1 (one) person. Thus, the TNH_{PSMIS} is calculated in the following manner:

$$ANHPP_{PSMIS} = \frac{4 \text{ hours}}{1 \text{ person}} = \frac{4 \text{ hours}}{\text{person}}$$

$$TNH_{PSMIS} = (ANHPP_{PSMIS})(NP_{PSMIS}) = \left(\frac{4 \text{ hours}}{\text{person}} \right) (1 \text{ person}) = 4 \text{ hours}$$

Therefore, by replacing the $TNH_{Manually}$ and TNH_{PSMIS} values into Equation 4.2 yields as follows:

$$E = 1 - \left(\frac{TNH_{PSMIS}}{TNH_{Manually}} \right) = 1 - \left(\frac{4 \text{ hours}}{300 \text{ hours}} \right) = 0.9867 = 98.67 \%$$

Table 4.3 recapitulates the KSC information of the time and manpower required to terminate the project manually and with the aid of the PSMIS.

Table 4.3: Summary of the efficiency elements for the KSC project.

Element	Manually	PSMIS
Avg. hours worked per person ($ANHPP$)	100	4
Persons involved in project (NP)	3	1
Total hours to complete project (TNH)	300	4
Efficiency of the PSMIS (E)	98.67 %	

Chapter 5

5. CONCLUSIONS AND RECOMMENDATIONS

After implementing and evaluating the PSMIS, some deductions can be drawn as well as some suggestions for future research. This chapter provides the conclusions and recommendations pertaining to the research done and described in this project about the development of a predictive safety management information system (PSMIS). This management information system (MIS) comprises the theory of the Continuous Hazard Tracking Failure Prediction Methodology (CHTFPM).

5.1 Introduction

The overview of this chapter is defined in this passage. Section 5.2 supplies a summary of the work performed. In Section 5.3, the conclusions about the results of this study are exposed while Section 5.4 discusses the potential implementation problems with the PSMIS. To finish, Section 5.5 presents the recommendations for future studies with the CHTFPM MIS/PSMIS.

5.2 Summary of Work Performed

The existing accident prevention models—like the ones revealed in Section 2.5.1—are either reactive or proactive in nature; however, not all of them are available in

a software application. The CHTFPM is a preventative safety model that is proactive, and it has been incorporated into a software package. By proactive, it is meant that corrective action is taken before the fact, instead of after the fact, in order to prevent an accident or system malfunction before occurring. To perform safety in a proactive manner, the CHTFPM combines the principles of safety sampling and control charts. Therefore, the CHTFPM MIS have these two previous concepts integrated, so that the safety status of a given system or process can be known. Besides the PSMIS, there are some predictive safety models that are proactive and exist in the form of a software system (refer to Section 2.6.2.1 and 2.6.2.2). Nonetheless, the disadvantage of these computer programs is that they are only applicable to specific sites or scenarios; whereas the CHTFPM MIS is robust, meaning that it is suitable for many locations, circumstances and studies.

In order to facilitate the application of the PSMIS and at the same time provide proof of the reliability and efficiency of the software, two previously validated case studies were selected. These two predictive safety projects were the following:

1. Promoted combustion testing operations at the Material and Combustion Research Facility at Marshall Space Flight Center (MSFC).
2. Testing, preparation and hoisting operation of four high-pressure gas tanks (HPGTs) at the Operations and Check-Out Building at Kennedy Space Center (KSC).

The two studies depicted above were chosen for the implementation of the CHTFPM MIS. This signifies that all the information encompassed in both projects was input into the PSMIS to verify if the results given by the software were the same as those obtained

by hand. By doing so, the confidence in the results of the CHTFPM code could be determined as well as the time necessary to complete the projects when the CHTFPM MIS was used relative to when it was not used. This provided the implementation and evaluation of the PSMIS.

5.3 Conclusions

The implementation and evaluation of the CHTFPM MIS on both case studies revealed the following inferences:

- For the MSFC case study, the results presented by the PSMIS for each control chart— c , weighted, EWMA ($L=3.054$, $\lambda=0.4$ and $L=2.814$, $\lambda=0.1$) and combined Shewhart-EWMA chart—are exactly the same as the ones attained manually.
- For the MSFC case study, the Pareto diagram produced by the PSMIS is identical to the one elaborated by the analyst.
- For the KSC case study, the results presented by the PSMIS for each control chart— c and weighted chart—match those obtained by hand.
- For the KSC case study, the Pareto diagram fabricated by the PSMIS is equal to the one constructed by the analyst.
- The PSMIS outcomes shown in Section 4.7 are evidence which undoubtedly supports that the CHTFPM software system is reliable and accurate.
- In the MSFC project, 3 persons were required to finish off the research manually resulting in 300 total number of hours ($TNH_{Manually}$) spent.

- In the MSFC project, 1 person completed the study in 3 hours ($TNH_{PSMIS} = 3$) using the PSMIS.
- In the MSFC project, there was a significant improvement in utilizing the CHTFPM MIS versus doing the project manually, for the efficiency of the PSMIS was 99 %.
- In the KSC case study, it took 3 persons to conclude the research study for a total number of hours ($TNH_{Manually}$) of 300.
- In the KSC case study, 1 person finalized the project in 4 hours ($TNH_{PSMIS} = 4$).
- In the KSC case study, there was a significant improvement in utilizing the CHTFPM MIS versus doing the research manually, for the efficiency of the PSMIS was 98.67 %.

5.4 Potential Implementation Problems

The possible problems that could be faced when implementing or applying the PSMIS are mainly related to collecting and, consequently, entering the data into the CHTFPM MIS. This is true because the management of data, especially the calculations, is handled by the computer program and not by the analyst. So, the program cannot give incorrect results unless the user makes a mistake. For instance, when constructing a Pareto diagram by manual means, the analyst can accidentally interchange the names of the dendritics at the moment of assigning them to their respective frequencies (bars). This would lead to wrong results and erroneous conclusions. Some of these potential problems are described in the following list of points:

- The accuracy of the responses given by the PSMIS depends on the precision with which the dendritic occurrences are entered. At the time of inputting such information, the analyst can indicate by mistake that a certain dendritic occurred when in reality it did not. This would give a variation in the plotted value of the selected control chart or in the frequency of that dendritic in the Pareto diagram.
- When entering the number of dendritics observed into the PSMIS screens—which correspond to a certain observation number—where the dendritic incidences are typed in, the user can accidentally skip one or more observation numbers (screens).
- If an inspection screen was not filled out on purpose because no dendritics occurred in that observation, the CHTFPM MIS will assume that such observation was not conducted and will not be considered for any associated calculations, such as sample size, control limits, plotted subgroup value, *etc* (review Section 3.8.2 to avoid this kind of problem).
- The analyst can forget to conduct an observation to check for the presence of dendritics in the system or can forget to input the dendritic occurrences into the CHTFPM system. Therefore, such observation number will be left in blank and will affect that particular subgroup size (refer to Section 3.8.2 to rectify this type of problem).
- If an inspection number is skipped in the PSMIS due to any of the reasons cited in this section, or for some other reason, it implies that not all the subgroups have the same sample size. As a consequence, the CHTFPM MIS will try to graph a \bar{u} chart by default, at the time of specifying which type of control chart to view, since this is

the only attribute chart that does not carry the restriction of equal sample size. The computer program, however, will display a warning/message before plotting the u chart (read Section 3.8.2 to learn how to correct this problem).

5.5 Future Research Recommendations

The goal of this research has been to devise a predictive safety software to control conditions leading to hazards from a proactive, instead of a reactive, standpoint. The CHTFPM MIS can be used as a starting point for future research to enhance the effectiveness of proactive safety projects. The recommendations for areas of future research include the following:

- Add to the PSMIS a multivariate EWMA (MEWMA) which can demonstrate a situation in which simultaneous monitoring and control of two or more related quality characteristics (variables) is necessary.
- Incorporate into the CHTFPM code the capability to perform a discriminant analysis to check the adequacy of the control charts and to generate an equation that could be utilized for prediction of system safety.
- Test and implement the PSMIS beta version (first edition) in other NASA facilities where the collection of data would be carried out in a real-time basis, hence in live industrial scenarios. This would serve to further validate the PSMIS (based on user input) and improve the usability of the CHTFPM MIS.

References

1. Bologna, Sandro and Hollnagel, Erik, 2002. Human-computer system dependability, Computer Safety, Reliability and Security—Stuart Anderson, Sandro Bologna and Massimo Felici, Eds.—(21st International Conference, *SAFECOMP*), pp. 1-3, Springer.
2. Borror, C. M.; Champ, C. W. and Rigdon, S. E., 1998. Poisson EWMA control charts, *Journal of Quality Technology*, Vol. 30, No. 4, pp. 352-361.
3. BSI, 1991. British Standard Institution. Reliability of Systems, Equipments and Components: Part 5 Guide to Failure Modes, Effects and Critically Analysis, BS 5760.
4. Chelbi, A. and Ait-Kadi, D., 1998. Inspection and predictive maintenance strategies, *International Journal of Computer-Integrated Manufacturing*, Vol. 11, pp. 226-231.
5. Cheng, Min-Yuan; Ko, Chien-Ho and Chang, Chih-Hung, 2002. Computer-aided DSS for safety monitoring of geotechnical construction, *Automation in Construction*, Vol. 11, pp. 375-290.
6. Cooper, J., 1998. Portraying information about sources of data in probabilistic analyses, *Proceedings of the 1998 ASME/JSME Joint Pressure Vessels and Piping Conference*. Vol. 378, pp. 26-30.
7. Dale, C. J. and Foster, S., 1987. The development of techniques for safety and reliability assessment: past, present and future, *Achieving Safety and Reliability*

- with Computer Systems—Edited by B. K. Daniels—(*Proceedings of the Safety and Reliability Society Symposium*), pp. 141-151, Elsevier Applied Science.
8. Davies, N.; Marriott, J.M.; Wightman, D.W. and Bendell, A., 1987. The musa data revisited: alternative methods and structure in software reliability modeling and analysis, *Achieving Safety and Reliability with Computer Systems*—Edited by B. K. Daniels—(*Proceedings of the Safety and Reliability Society Symposium*), pp. 118-130, Elsevier Applied Science.
 9. Devore, Jay L., 1995. Probability and Statistics for Engineering and the Sciences, 4th Edition, Wadsworth, Inc., Belmont, CA.
 10. Font, V., 1985. Une approche de la fiabilité des logiciels: modèles classiques et modèle linéaire généralisé, *Ph.D. Thesis, L'Université Paul Sabatier de Toulouse*, France.
 11. Grant, E. L. and Leavenworth, R. S., 1996. Statistical Quality Control, McGraw-Hill, Inc., New York, NY.
 12. Greibe, Poul, 2002. Accident prediction models for urban roads, *Accident Analysis and Prevention*, Vol. 839, pp. 1-13.
 13. Greibe, P. and Hemdorff, S., 1995. Uheldsmodel for bygader-Del1: Modeller for 3-og 4-benede kryds. Notat 22, The Danish Road Directorate.
 14. Greibe, P. and Hemdorff, S., 1998. Uheldsmodel for bygader-Del2: Modeller for strækninger. Notat 59, The Danish Road Directorate.
 15. Grimaldi, J. V. and Simonds, R. H., 1989. Safety Management, 5th Edition, Boston, MA.

16. Guria, Jagadish and Mara, Kelly, 2000. Monitoring performance of road safety programmes in New Zealand, *Accident Analysis and Prevention*, Vol. 32, pp. 695-702.
17. HSC, 1992. Health and Safety Commission. Management of Health and Safety at Work Regulations, HSC Approved Code of Practice, ISBN 0-11-886330-4.
18. Hunter, J. S., 1986. The exponentially weighted moving average, *Journal of Quality Technology*, Vol. 18, No. 4, pp. 203-210.
19. Johnson, W., 1995. Nuclear plant maintenance: NMAC's perspective, *Proceedings of the American Power Conference*, Vol. 57, pp. 514-518.
20. Juran, J. M. and Gryna, F. M., Eds., 1988. Juran's Quality Control Handbook, 4th Edition, McGraw-Hill, Inc., New York, NY.
21. Kaâniche, Mohamed; Laprie, Jean-Claude and Blanquart, Jean-Paul, 2002. A framework for dependability engineering of critical computing systems, *Safety Science*, Vol. 40, pp. 731-752.
22. Kaplan, S., 1991. Risk Assessment and Risk Management – Basic Concepts and Terminology, Hemisphere Publishing, New York, NY.
23. Kolarik, William J., 1999. Creating Quality: Process Design for Results, McGraw-Hill Companies, Inc, New York, NY.
24. Koval, D. O., 1997. Human element factors affecting reliability and safety, *Record of Industrial and Commercial Power Systems Technical Conference*, pp. 14-21.
25. Lee, Charles; Garnsworthy, Jon; Chudleigh, Morris and Bishop, Duncan, 1998. Issues in managing a safety-critical system development project, *Industrial Perspectives*

- of Safety-critical Systems—Edited by Felix Redmill and Tom Anderson—
(*Proceedings of the Sixth Safety-critical Systems Symposium*), pp. 1-26, Springer.
26. Levinson, W. A. and Tumbelty, F., 1997. SPC Essentials and Productivity Improvement: A Manufacturing Approach, ASQC Quality Press, Milwaukee, WI.
 27. Lucas, J. M. and Saccucci, M. S., 1990. Exponentially weighted moving average control schemes: properties and enhancements, *Technometrics*, Vol. 32, No. 1, pp. 1-29.
 28. Mackie, R.I., 1998. An object-oriented approach to fully interactive finite element software, *Advances in Engineering Software*, Vol. 29, No. 2, pp. 139-149.
 29. Mackie, R.I., 2001. Implementation of sub-structuring within an object-oriented framework, *Advances in Engineering Software*, Vol. 32, pp. 749-758.
 30. Mangonon, Pat L., 1999. The Principles of Materials Selection for Engineering Design, Prentice-Hall, New Jersey.
 31. Marcombe, J. T., 1993. Behavior-based safety at Monsanto's Pensacola plant, *Chemical Engineer (London)*, No. 541, pp. 15-17.
 32. Marshall, G., 1982. Safety Engineering, Brooks/Cole Engineering Division, Monterey, CA.
 33. Martin, James, 1987. Recommended Diagramming Standards for Analysts & Programmers: A Basis for Automation, Prentice-Hall, Inc., Englewood Cliffs, NJ.
 34. Meister, D., 1985. Behavioral Analysis and Measurement Methods, John Wiley and Sons, New York, NY.

35. Montgomery, Douglas C., 1996. Introduction to Statistical Quality Control, 3rd Edition, John Wiley and Sons, New York, NY.
36. Nagel, P.M. and Skrivan, J.A., 1981. Software reliability: repetitive run experimentation and modeling, *Boeing Computer Services Co. Report, BLS-40366*, NASA report No. CR-165836.
37. Ng, C. H. and Case, K. E., 1989. Development and evaluation of control charts using exponentially weighted moving averages, *Journal of Quality Technology*, Vol. 21, No. 4, pp. 242-250.
38. Norin, Hans and Isaksson-Hellman, Irene, 1995. Injury potential prediction of a safety design feature: A theoretical method based on simulations and traffic accident data, *Safety Science*, Vol. 19, pp. 45-56.
39. Norin, H.; Jernström, C.; Koch, M.; Ryrberg, S. and Svensson, S-E., 1991. Avoiding suboptimized occupant safety by multiple speed impact testing, *13th ESV Conf.*, Paris, pp. 1-17, Paper No. 91-S9-O-89.
40. Olsen, D. A., 1993. CEO's Can Reform Workers' Compensation, *The New York Times*, January 3, New York, NY.
41. Preyssl, C., 1995. Safety risk assessment and management – the ESA approach, *Reliability Engineering and System Safety*, Vol. 49, pp. 303-309.
42. Quintana, R., Camet, M. and Deliwala, B., 2001. Application of a predictive safety model in a combustion testing environment, *Safety Science*, Vol. 38, pp. 183-209.
43. Roland, H.E. and Moriarity, B., 1983. System Safety Engineering and Management, John Wiley and Sons, New York, NY.

44. Ryan, T. P., 1989. Statistical Methods for Quality Improvement, John Wiley and Sons, New York, NY.
45. Shell, R. L., Ed., 1986. Work Measurement: Principles and Practice, Industrial Engineering and Management Press, Atlanta, GA.
46. Spalding, Ian, 1998. Principles of engineering safety management, Industrial Perspectives of Safety-critical Systems—Edited by Felix Redmill and Tom Anderson—(*Proceedings of the Sixth Safety-critical Systems Symposium*), pp. 27-43, Springer.
47. TNO Road-Vehicle Research Institute, 1990. MADYMO, Databases, Version 4.3, The Netherlands.
48. TNO Road-Vehicle Research Institute, 1990. MADYMO, Users Manual 3D, Version 4.3, The Netherlands.
49. Veevers, A.; Petrova, E. and Marshall, A. C., 1987. Statistical methods for software reliability assessment, past, present and future, Achieving Safety and Reliability with Computer Systems—Edited by B. K. Daniels—(*Proceedings of the Safety and Reliability Society Symposium*), pp. 141-151, Elsevier Applied Science.
50. Vining, G. G., 1998. Statistical Methods for Engineers, Duxbury Press, New York, NY.
51. Whitten, Jeffrey L.; Bentley, Lonnie D. and Barlow, Victor M., 1989. Systems Analysis & Design Methods, 2nd Edition, Richard D. Irwin, Inc., Boston, MA.

52. Wightman, D. W. and Bendell, A., 1986. Proportional hazards modeling of software failure data, *Software Reliability, State of the Art Report*, 14:2, pp. 230-242, Pergamon Infotech, Oxford.
53. Williams, B., 1978. *A Sampler on Sampling*, John Wiley and Sons, New York, NY.
54. Wilson, P. F.; Dell, L.D. and Anderson, G. F., 1993. *Root Cause Analysis: A Tool for Total Quality Management*, ASQ Quality Press, Milwaukee, WI.
55. Wise, S. A. and Fair, D. C., 1998. *Innovative Control Charting*, ASQC Quality Press, Chicago, IL.
56. Wrench, Constance P., 1990. *Data Management for Occupational Health and Safety: A User's Guide to Integrating Software*, Van Nostrand Reinhold, New York, NY.
57. Zissler, J., 1996. Predictive hydraulic maintenance, *Occupational Health and Safety*, Vol. 65, pp. 62-65.

Glossary

ARL: *Average Run Length*, the expected number of sampling stages before an out-of-control condition is raised.

Barrier Analysis: Examines any root cause of a given problem or unwanted event by assessing the adequacy of any installed barriers, like safeguards, that can prevent an accident or system failure.

Binomial Distribution: It is used frequently in statistical process control. It is the appropriate probability model for sampling from an infinitely large population, where the fraction of defective or nonconforming items in the population or sample are of interest.

BSI: *British Standards Institution*, group of complementary business—all working to the same vision of supporting business improvement and trade worldwide.

CHTFPM: *Continuous Hazard Tracking and Failure Prediction Methodology*, a proactive predictive safety model that aids in preventing accidents and system failures.

CHTFPM MIS: See PSMIS.

Center Line: Process mean obtained based on the selected attribute or Shewhart control chart.

Confidence Interval: An interval of plausible values for the parameter being estimated.

Confidence Level: Degree of plausibility or chance that a confidence interval has of including the universe.

Control Chart: A simple graphical device for knowing, at a given instance of time, whether or not a process is under control.

Demerit Scheme: Method of assigning demerits or weights to dendritics or problems according to their severity.

Dendritics: Building blocks of hazards or conditions in a given system that are becoming hazardous.

DSS: *Decision Support System*, a safety computer system designed to assist construction engineers in monitoring and controlling the excavation conditions that could become hazardous in construction sites.

FMEA: *Failure Mode and Effect Analysis*, is a bottom-up hazard analysis procedure of identifying the failure modes of a system and determining the effects on the next higher level.

Frequency: The tally or count of only the number of observations associated with each object or item (dendritic, problem, individual, *etc.*)

Hazard: The potential for an activity, condition, or circumstance to produce harmful effects.

Hazard Analysis: The process of identifying, anticipating and controlling hazards.

HSE: *Health and Safety Executive*, responsible for the regulation of almost all the risks to health and safety arising from work activity in Great Britain.

LCL: *Lower Control Limit*, delineates the bottom safety boundary in a control chart for a given system or process.

MADYMO: Mathematical simulation models that can predict type of injuries in a certain car accident configuration before the system (human) is exposed to harmful circumstances.

Mean: The sum of values in a distribution divided by the number of values. It is one of the most common measures of central tendency.

MIS: *Management Information System*, computer application that is capable of organizing, storing and retrieving information.

Normal Distribution: A bell shaped distribution which describes most of the naturally occurring phenomena. A normal distribution is identified by the mean and standard deviation.

OSHA: *Occupational Safety and Health Administration*, an organization within the Department of Labor, with a mission to ensure that every employer provides safe and healthful conditions to every working man and woman.

Parameter: A constant or coefficient of a universe that describes some characteristic of its distribution.

Pareto Analysis: A technique for prioritizing types or sources of problems by separating the major causes from the minor causes of a problem (dendritics). This allows for a focus on problems that offer the greatest potential for process improvement by using a Pareto chart of diagram.

Pareto Chart: Also known as Pareto diagram. It is a bar graph that represents the frequencies of dendritics or problems.

Percent Error: Desired or specified α , this is the probability of data falling outside the confidence level.

PHA: *Preliminary Hazard Analysis*, is a system safety analysis tool which identifies critical safety areas, evaluates hazards, and identifies the safety design criteria to be used in order to eliminate or reduce the risk.

Poisson Distribution: It is a typical application in statistical process control. It is a model of the number of defects or nonconformities that occur in a unit or product. In fact, any random phenomenon that occurs on a per unit (or per unit area, per unit volume, per unit time, *etc.*) basis is often well approximated by the Poisson distribution.

Population: See universe.

Probability: The proportion of an object or thing (dendritic, problem, *etc.*) in a given class, group, collection or set or data.

PSMIS: *Predictive Safety Management Information System*, software package that incorporates the theory of the CHTFPM and performs data handling, data manipulation as well as calculations automatically.

Random: An intuitive concept referring to a condition that happens unpredictably and without any apparent pattern or reason. Equal chance of probability of occurrence for each member of a group.

Risk: A measure of both the likelihood and consequences of all hazards of an activity or condition. It is the chance of injury, damage or loss.

Risk Analysis: Method of applying qualitative and quantitative techniques to measure potential risk in terms of frequency and severity rate.

Safety: Is the state of being relatively free from harm, danger, injury or damage.

Safety Engineering: Is the application of engineering principles to the recognition and control of hazards.

Safety Sampling: A proactive approach for accident and system failure prevention by monitoring the occurrence of dendritics in order to determine if a system is operating within the specified control limits.

Sample: Portion or subset of objects or items from a larger set called universe.

Sampling: The activity of picking a sample from a universe to draw inferences about the universe.

Significance: Means that a result differs from or exceeds some hypothetical value by more than it can reasonably be attributed to the chance errors of sampling.

Standard Deviation: The measure of the dispersion of the observed values about their mean.

UCL: *Upper Control Limit*, delineates the top safety boundary in a control chart for a given system or process.

Universe: The set of all individuals or objects of a particular type.

APPENDIX A

Preliminary Hazard Analysis for the MSFC Project

PRELIMINARY HAZARD ANALYSIS				
Hazardous Condition	Hazard Cause	Hazard Effect	Safety/Engineering Requirements	Hazard Elimination/ Control Provisions
Expired calibration (gauge, transducer, etc.)	Human error (scheduling)	Loss of confidence in component indication	Meet minimum calibration requirements as specified by manufacturer	Calibration schedule reviews and audits
Component missing part #, hydrostat information, manufacturer information, or specifications (hose, valve, etc.)	Workmanship	Unable to identify critical component characteristics	All hoses and valves must maintain required id and equipment specifications readily viewable	Periodic walkthrough/inspection, attach new tags with necessary information
Component id information covered by paint (hose, valve, manifold, etc.)	Workmanship	Unable to identify critical component characteristics	All hoses and valves must maintain required id and equipment specifications readily viewable	Periodic walkthrough/inspection, remove paint from id tags
Maintenance performed incorrectly	Workmanship	Inoperative equipment or deficient system operation	Maintenance conducted according to NASA regulations	Properly trained maintenance technicians with sufficient oversight from maintenance supervisors
Implementation of newly designed equipment/system	Design deficiency	Inoperative equipment or deficient system operation	Design of systems to meet applicable NASA operational and safety requirements	Engineering review of all new design projects to ensure compliance and operational integrity
Equipment operator incorrectly operating equipment	Human error	Personnel risk, equipment damage, delay in operations	Design of equipment to be user friendly and operator foolproof	Equipment operator use SOPs posted at equipment being operated

APPENDIX B

Failure Mode and Effect Analysis for the MSFC Project

Find No. / Part No.	Part Name	Part Function	A. FAILURE MODE B. CAUSE C. FAILURE MODE NUMBER D. DETECTION METHOD E. CORRECTING ACTION F. TIME TO EFFECT G. TIMEFRAME	Failure Effect on System Performance	Failure Effects on Systems and / or Personnel Safety	Crit
N / A	Calibration Technician	Performs calibration of assigned equipment (gauges, transducers, etc)	A. Fails to calibrate equipment by due date B. Scheduling D. Inspection of calibration records, visible discrepancy in equipment, etc... E. Calibrate F. Varying G. Yet to be determined	<input type="checkbox"/> Loss of confidence in equipment indication / operation <input type="checkbox"/> Possible failure cause in function / use / operation of equipment or system <input type="checkbox"/> Possible factor in equipment downtime and / or life expectancy	Possible effects include minor to severe personnel risks, system component failure, system failure	3
N / A	Lubrication Technician	Lubricates all rotors, rings and other parts needing lubrication	A. Fails to lubricate B. Scheduling, negligence / oversight D. Inspection of maintenance records, visible discrepancy in equipment, etc... E. Lubricate F. Varying G. Yet to be determined	<input type="checkbox"/> Possible failure cause in function / use / operation <input type="checkbox"/> Possible factor in equipment downtime and / or life expectancy <input type="checkbox"/> Loss of confidence in equipment indication / operation	Possible effects include minor to severe personnel risks, system component failure, system failure	3
N / A	Post-Test System Operator	Equipment shutdown inspection, clean-up and similar post-operational tasks	A. Fails to properly shutdown, inspect, clean-up equipment and/or its components B. Human error / oversight D. Operational problem / failure safety infringement recognition / discrepancy E. Increase adherence to post-test procedures guidelines and/or checklists, enlarged focus on safety standards, etc. F. Varying G. Yet to be determined	<input type="checkbox"/> Possibility of multiple effects ranging from minor to major equipment failure / hazard and / or component failure / hazard	Possible effects include minor to severe personnel risks, system component failure, system failure	3

Find No./ Part No.	Part Name	Part Function	A. FAILURE MODE B. CAUSE C. FAILURE MODE NUMBER D. DETECTION METHOD E. CORRECTING ACTION F. TIME TO EFFECT G. TIME FRAME	Failure Effect on System Performance	Failure Effects on Systems and / or Personnel Safety	Crit
N / A	Sample Technician / Handler	Prepares, loads, unloads and / or handles test samples	A. Fails to properly prepare, load, unload and / or handle test samples as well as tabulating sample information B. Possible causes include human error / oversight, chemical impotency, mechanical malfunction of parts related to loading / unloading of samples, measurement of sample properties and so on D. Notable abnormality of sample or sample handling, discrepancy in sample data sheets, improper sample situation in chamber E. Prepare sample again or acquire new sample, re-load sample, improved adherence to procedural guidelines in sample preparation, loading and handling F. Varying G. Yet to be determined	<input type="checkbox"/> Possibility of multiple effects ranging from minor to major equipment failure / hazard and / or component failure / hazard	Possible effects include personnel risks, system component failure, system failure, test biasing and sample corruption	3
N / A	Maintenance Technician	Performs corrective and / or predictive maintenance	A. Incorrectly performs maintenance B. Workmanship D. Inspection of maintenance records, visible discrepancy in equipment, etc. E. Perform the maintenance tasks F. Varying G. Yet to be determined	<input type="checkbox"/> Loss of confidence in equipment indication / operation	Possible effects include minor to severe personnel risks, system component failure, system failure	3
N / A	Electrical System Components	Electrical connections, components	A. Improper function / use / connection of electrical apparatus and electronic components B. Various D. Visual or functional discrepancy of equipment and / or its components E. Repair or replacement of faulty part / apparatus F. Varying G. Yet to be determined	<input type="checkbox"/> Loss of confidence in equipment indication / operation <input type="checkbox"/> Possible failure cause in function / use / operation of equipment or system <input type="checkbox"/> Possible factor in equipment downtime and / or life expectancy	Possible effects include minor to severe personnel risks, system component failure, system failure	3

Find No. / Part No.	Part Name	Part Function	A. FAILURE MODE B. CAUSE C. FAILURE MODE NUMBER D. DETECTION METHOD E. CORRECTING ACTION F. TIME TO EFFECT G. TIMESCALE	Failure Effect on System Performance	Failure Effects on Systems and / or Personnel Safety	Crit
N / A	Mechanical System Components	Seals, valves, plugs, insulation and other functionally similar components	A. Improper function / use / connection of components mentioned at left B. Various D. Visual or functional discrepancy of equipment and / or its components E. Repair or replacement of faulty part / apparatus F. Varying G. Yet to be determined	<input type="checkbox"/> Loss of confidence in equipment indication / operation <input type="checkbox"/> Possible failure cause in function / use / operation of equipment or system <input type="checkbox"/> Possible factor in equipment downtime and / or life expectancy	Possible effects include minor to severe personnel risks, system component failure, system failure	3
N / A	Mechanical System Components	Knobs, buttons, switches, gauges, and other functionally similar components	A. Improper function / use / connection of components mentioned at left B. Various D. Visual or functional discrepancy of equipment and / or its components E. Repair or replacement of faulty part / apparatus F. Varying G. Yet to be determined	<input type="checkbox"/> Loss of confidence in equipment indication / operation <input type="checkbox"/> Possible failure cause in function / use / operation of equipment or system <input type="checkbox"/> Possible factor in equipment downtime and / or life expectancy	Possible effects include minor to severe personnel risks, system component failure, system failure	3
N / A	Electrical System Components	ViewDac and other computer devices	A. Improper function / use / of computer applications, malfunctioning components, both software and hardware B. Various D. Inoperable or malfunctioning system related to a computer application, malfunctioning computer exercise or package E. If unqualified, contact more suitable technician; if ViewDac, contact manufacturer F. Varying G. Yet to be determined	<input type="checkbox"/> Loss of system monitoring, control and / or applications	Possible effects include minor to severe personnel risks, system component failure, system failure	3
N / A	Mechanical System Components	Compressors, lift plates and other functionally similar components	A. Improper function / use / connection of components mentioned at left B. Various D. Visual or functional discrepancy of equipment and / or its components E. Repair or replacement of faulty part / apparatus F. Varying G. Yet to be determined	<input type="checkbox"/> Loss of confidence in equipment indication / operation <input type="checkbox"/> Possible failure cause in function / use / operation of equipment or system <input type="checkbox"/> Possible factor in equipment downtime and / or life expectancy	Possible effects include minor to severe personnel risks, system component failure, system failure	3

APPENDIX C

Barrier Analysis for the MSFC Project

Target	Threat	Barrier	Analysis
Personnel	Back Injury	Training on general safe lab practices	Incorrect posture used
Personnel	Oxygen Bottle Explosion	Training on proper handling of compressed gas cylinders	Occasional violation of handling procedures
Personnel	Eye Injury	Training on use of personal protection equipment , required to wear safety glasses	Intermittent violation of PPE requirements
Personnel	Burn Injury	Ceramic cup to catch slag	Used for all testing operations, emptied intermittently
Personnel	Foot Injury	Training on use of personal protection equipment , required to wear safety shoes	Intermittent violation of PPE requirements

APPENDIX D

c Control Chart Data for the MSFC Project

Sample	Number of Dendritics Observed (c)	Sample	Number of Dendritics Observed (c)
1	0	51	3
2	1	52	1
3	2	53	1
4	1	54	1
5	1	55	0
6	3	56	2
7	4	57	3
8	4	58	3
9	3	59	1
10	2	60	2
11	2	61	3
12	1	62	3
13	3	63	2
14	2	64	2
15	2	65	2
16	0	66	7
17	0	67	3
18	0	68	3
19	1	69	3
20	1	70	1
21	1	71	4
22	1	72	2
23	1	73	2
24	2	74	2
25	1	75	2
26	0	76	3
27	0	77	0
28	4	78	2
29	0	79	2
30	0	80	3
31	1	81	0
32	1	82	0
33	0	83	0
34	1	84	1
35	1	85	1
36	1	86	2
37	1	87	2
38	0	88	2
39	0	89	4
40	1	90	3
41	0	91	3
42	0	92	0
43	0	93	4
44	2	94	4
45	2	95	1
46	2	96	0
47	3	97	0
48	3	98	0
49	0	99	0
50	7	100	0

APPENDIX E

Weighted Control Chart Data for the MSFC Project

Sample	Class A	Class B	Class C	Class D	D_{ij}	u_{ij}	\bar{u}_A	\bar{u}_B	\bar{u}_C	\bar{u}_D
1	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
2	1	0	0	0	100	25.00	0.25	0.00	0.00	0.00
3	2	0	0	0	200	50.00	0.50	0.00	0.00	0.00
4	1	0	0	0	100	25.00	0.25	0.00	0.00	0.00
5	0	0	1	0	10	2.50	0.00	0.00	0.25	0.00
6	0	1	2	0	70	17.50	0.00	0.25	0.50	0.00
7	0	1	3	0	80	20.00	0.00	0.25	0.75	0.00
8	0	1	3	0	80	20.00	0.00	0.25	0.75	0.00
9	0	1	2	0	70	17.50	0.00	0.25	0.50	0.00
10	0	0	2	0	20	5.00	0.00	0.00	0.50	0.00
Preliminary Sampling Study							\bar{u}_A	\bar{u}_B	\bar{u}_C	\bar{u}_D
							0.10	0.10	0.325	0.00
Sample	Class A	Class B	Class C	Class D	D_{ij}	u_{ij}	\bar{u}_A	\bar{u}_B	\bar{u}_C	\bar{u}_D
11	0	0	2	0	20	5.00	0.00	0.00	0.50	0.00
12	0	1	0	0	50	12.50	0.00	0.25	0.00	0.00
13	0	0	3	0	30	7.50	0.00	0.00	0.75	0.00
14	0	0	2	0	20	5.00	0.00	0.00	0.50	0.00
15	0	0	2	0	20	5.00	0.00	0.00	0.50	0.00
16	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
17	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
18	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
19	0	0	1	0	10	2.50	0.00	0.00	0.25	0.00
20	1	0	0	0	100	25.00	0.25	0.00	0.00	0.00
21	1	0	0	0	100	25.00	0.25	0.00	0.00	0.00
22	0	0	1	0	10	2.50	0.00	0.00	0.25	0.00
23	0	0	1	0	10	2.50	0.00	0.00	0.25	0.00
24	0	1	1	0	60	15.00	0.00	0.25	0.25	0.00
25	0	0	1	0	10	2.50	0.00	0.00	0.25	0.00
26	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
27	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
28	0	0	4	0	40	10.00	0.00	0.00	1.00	0.00
29	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
30	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
31	0	1	0	0	50	12.50	0.00	0.25	0.00	0.00
32	0	1	0	0	50	12.50	0.00	0.25	0.00	0.00
33	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
34	0	0	1	0	10	2.50	0.00	0.00	0.25	0.00
35	0	0	1	0	10	2.50	0.00	0.00	0.25	0.00
36	0	1	0	0	50	12.50	0.00	0.25	0.00	0.00
37	0	0	1	0	10	2.50	0.00	0.00	0.25	0.00
38	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
39	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
40	0	0	1	0	10	2.50	0.00	0.00	0.25	0.00
41	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
42	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
43	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
44	0	0	2	0	20	5.00	0.00	0.00	0.50	0.00
45	0	0	2	0	20	5.00	0.00	0.00	0.50	0.00
46	0	1	1	0	60	15.00	0.00	0.25	0.25	0.00
47	1	1	1	0	160	40.00	0.25	0.25	0.25	0.00
48	1	0	2	0	120	30.00	0.25	0.00	0.50	0.00
49	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00

Sample	Class A	Class B	Class C	Class D	D_i	U_i	U_{ij}	U_{ij}^2	U_{ij}^3	U_{ij}^4
50	1	2	4	0	240	60.00	0.25	0.50	1.00	0.00
51	0	0	3	0	30	7.50	0.00	0.00	0.75	0.00
52	1	0	0	0	100	25.00	0.25	0.00	0.00	0.00
53	1	0	0	0	100	25.00	0.25	0.00	0.00	0.00
54	1	0	0	0	100	25.00	0.25	0.00	0.00	0.00
55	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
56	0	0	2	0	20	5.00	0.00	0.00	0.50	0.00
57	2	0	1	0	210	52.50	0.50	0.00	0.25	0.00
58	3	0	0	0	300	75.00	0.75	0.00	0.00	0.00
59	0	0	1	0	10	2.50	0.00	0.00	0.25	0.00
60	0	0	2	0	20	5.00	0.00	0.00	0.50	0.00
61	2	0	1	0	210	52.50	0.50	0.00	0.25	0.00
62	3	0	0	0	300	75.00	0.75	0.00	0.00	0.00
63	2	0	0	0	200	50.00	0.50	0.00	0.00	0.00
64	0	0	2	0	20	5.00	0.00	0.00	0.50	0.00
65	0	1	1	0	60	15.00	0.00	0.25	0.25	0.00
66	3	0	4	0	340	85.00	0.75	0.00	1.00	0.00
67	0	1	2	0	70	17.50	0.00	0.25	0.50	0.00
68	0	1	2	0	70	17.50	0.00	0.25	0.50	0.00
69	0	0	3	0	30	7.50	0.00	0.00	0.75	0.00
70	0	0	1	0	10	2.50	0.00	0.00	0.25	0.00
71	3	0	1	0	310	77.50	0.75	0.00	0.25	0.00
72	2	0	0	0	200	50.00	0.50	0.00	0.00	0.00
73	0	0	2	0	20	5.00	0.00	0.00	0.50	0.00
74	1	0	1	0	110	27.50	0.25	0.00	0.25	0.00
75	2	0	0	0	200	50.00	0.50	0.00	0.00	0.00
76	2	0	1	0	210	52.50	0.50	0.00	0.25	0.00
77	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
78	1	0	1	0	110	27.50	0.25	0.00	0.25	0.00
79	1	0	1	0	110	27.50	0.25	0.00	0.25	0.00
80	0	0	3	0	30	7.50	0.00	0.00	0.75	0.00
81	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
82	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
83	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
84	0	0	1	0	10	2.50	0.00	0.00	0.25	0.00
85	0	0	1	0	10	2.50	0.00	0.00	0.25	0.00
86	0	0	2	0	20	5.00	0.00	0.00	0.50	0.00
87	0	0	2	0	20	5.00	0.00	0.00	0.50	0.00
88	0	1	1	0	60	15.00	0.00	0.25	0.25	0.00
89	0	0	4	0	40	10.00	0.00	0.00	1.00	0.00
90	0	0	3	0	30	7.50	0.00	0.00	0.75	0.00
91	0	0	3	0	30	7.50	0.00	0.00	0.75	0.00
92	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
93	0	0	4	0	40	10.00	0.00	0.00	1.00	0.00
94	0	1	3	0	80	20.00	0.00	0.25	0.75	0.00
95	1	0	0	0	100	25.00	0.25	0.00	0.00	0.00
96	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
97	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
98	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
99	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
100	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00

APPENDIX F

EWMA Control Chart Data for the MSFC Project ($\lambda = 0.4$, $L = 3.054$)

Sample	Subgroup value (n)	EWMA chart point (Z)	UCL	CL
1	0	1.26000	3.87027	0.32973
2	1	1.15600	4.16447	0.03553
3	2	1.49360	4.26060	-0.06060 = 0
4	1	1.29616	4.29417	-0.09417 = 0
5	1	1.17770	4.30613	-0.10613 = 0
6	3	1.90662	4.31042	-0.11042 = 0
7	4	2.74397	4.31197	-0.11197 = 0
8	4	3.24638	4.31252	-0.11252 = 0
9	3	3.14783	4.31272	-0.11272 = 0
10	2	2.68870	4.31279	-0.11279 = 0
11	2	2.41322	4.31282	-0.11282 = 0
12	1	1.84793	4.31283	-0.11283 = 0
13	3	2.30876	4.31283	-0.11283 = 0
14	2	2.18526	4.31283	-0.11283 = 0
15	2	2.11115	4.31283	-0.11283 = 0
16	0	1.26669	4.31283	-0.11283 = 0
17	0	0.76002	4.31283	-0.11283 = 0
18	0	0.45601	4.31283	-0.11283 = 0
19	1	0.85601	4.31283	-0.11283 = 0
20	1	0.91361	4.31283	-0.11283 = 0
21	1	0.94816	4.31283	-0.11283 = 0
22	1	0.96890	4.31283	-0.11283 = 0
23	1	0.98134	4.31283	-0.11283 = 0
24	2	1.38880	4.31283	-0.11283 = 0
25	1	1.23328	4.31283	-0.11283 = 0
26	0	0.73997	4.31283	-0.11283 = 0
27	0	0.44398	4.31283	-0.11283 = 0
28	4	1.86639	4.31283	-0.11283 = 0
29	0	1.11983	4.31283	-0.11283 = 0
30	0	0.67190	4.31283	-0.11283 = 0
31	1	0.80314	4.31283	-0.11283 = 0
32	1	0.88188	4.31283	-0.11283 = 0
33	0	0.52913	4.31283	-0.11283 = 0
34	1	0.71748	4.31283	-0.11283 = 0
35	1	0.83049	4.31283	-0.11283 = 0
36	1	0.89829	4.31283	-0.11283 = 0
37	1	0.93898	4.31283	-0.11283 = 0
38	0	0.56339	4.31283	-0.11283 = 0
39	0	0.33803	4.31283	-0.11283 = 0
40	1	0.60282	4.31283	-0.11283 = 0
41	0	0.36169	4.31283	-0.11283 = 0
42	0	0.21701	4.31283	-0.11283 = 0
43	0	0.13021	4.31283	-0.11283 = 0
44	2	0.87813	4.31283	-0.11283 = 0
45	2	1.32688	4.31283	-0.11283 = 0
46	2	1.59613	4.31283	-0.11283 = 0
47	3	2.15768	4.31283	-0.11283 = 0
48	3	2.49461	4.31283	-0.11283 = 0
49	0	1.49676	4.31283	-0.11283 = 0
50	7	3.69806	4.31283	-0.11283 = 0

Sample	Subgroup value (Z)	EWMA chart point (Z)	UCL	LCL
51	3	3.41883	4.31283	-0.11283 = 0
52	1	2.45130	4.31283	-0.11283 = 0
53	1	1.87078	4.31283	-0.11283 = 0
54	1	1.52247	4.31283	-0.11283 = 0
55	0	0.91348	4.31283	-0.11283 = 0
56	2	1.34809	4.31283	-0.11283 = 0
57	3	2.00885	4.31283	-0.11283 = 0
58	3	2.40531	4.31283	-0.11283 = 0
59	1	1.84319	4.31283	-0.11283 = 0
60	2	1.90591	4.31283	-0.11283 = 0
61	3	2.34355	4.31283	-0.11283 = 0
62	3	2.60613	4.31283	-0.11283 = 0
63	2	2.36368	4.31283	-0.11283 = 0
64	2	2.21821	4.31283	-0.11283 = 0
65	2	2.13092	4.31283	-0.11283 = 0
66	7	4.07855	4.31283	-0.11283 = 0
67	3	3.64713	4.31283	-0.11283 = 0
68	3	3.38828	4.31283	-0.11283 = 0
69	3	3.23297	4.31283	-0.11283 = 0
70	1	2.33978	4.31283	-0.11283 = 0
71	4	3.00387	4.31283	-0.11283 = 0
72	2	2.60232	4.31283	-0.11283 = 0
73	2	2.36139	4.31283	-0.11283 = 0
74	2	2.21684	4.31283	-0.11283 = 0
75	2	2.13010	4.31283	-0.11283 = 0
76	3	2.47806	4.31283	-0.11283 = 0
77	0	1.48684	4.31283	-0.11283 = 0
78	2	1.69210	4.31283	-0.11283 = 0
79	2	1.81526	4.31283	-0.11283 = 0
80	3	2.28916	4.31283	-0.11283 = 0
81	0	1.37349	4.31283	-0.11283 = 0
82	0	0.82410	4.31283	-0.11283 = 0
83	0	0.49446	4.31283	-0.11283 = 0
84	1	0.69667	4.31283	-0.11283 = 0
85	1	0.81800	4.31283	-0.11283 = 0
86	2	1.29080	4.31283	-0.11283 = 0
87	2	1.57448	4.31283	-0.11283 = 0
88	2	1.74469	4.31283	-0.11283 = 0
89	4	2.64681	4.31283	-0.11283 = 0
90	3	2.78809	4.31283	-0.11283 = 0
91	3	2.87285	4.31283	-0.11283 = 0
92	0	1.72371	4.31283	-0.11283 = 0
93	4	2.63423	4.31283	-0.11283 = 0
94	4	3.18054	4.31283	-0.11283 = 0
95	1	2.30832	4.31283	-0.11283 = 0
96	0	1.38499	4.31283	-0.11283 = 0
97	0	0.83100	4.31283	-0.11283 = 0
98	0	0.49860	4.31283	-0.11283 = 0
99	0	0.29916	4.31283	-0.11283 = 0
100	0	0.17950	4.31283	-0.11283 = 0

APPENDIX G

EWMA Control Chart Data for the MSFC Project ($\lambda = 0.1$, $L = 2.814$)

Sample	Subgroup value (Z)	EWMA chart point (Z)	UCL	LCL
1	0	1.89000	2.50779	1.69221
2	1	1.80100	2.64862	1.55138
3	2	1.82090	2.74038	1.45962
4	1	1.73881	2.80602	1.39398
5	1	1.66493	2.85501	1.34499
6	3	1.79844	2.89248	1.30752
7	4	2.01859	2.92158	1.27842
8	4	2.21673	2.94441	1.25559
9	3	2.29506	2.96247	1.23753
10	2	2.26555	2.97682	1.22318
11	2	2.23900	2.98827	1.21173
12	1	2.11510	2.99744	1.20256
13	3	2.20359	3.00480	1.19520
14	2	2.18323	3.01072	1.18928
15	2	2.16491	3.01548	1.18452
16	0	1.94842	3.01933	1.18067
17	0	1.75357	3.02243	1.17757
18	0	1.57822	3.02493	1.17507
19	1	1.67822	3.02695	1.17305
20	1	1.61040	3.02859	1.17141
21	1	1.54936	3.02991	1.17009
22	1	1.49442	3.03098	1.16902
23	1	1.44498	3.03185	1.16815
24	2	1.50048	3.03255	1.16745
25	1	1.45043	3.03311	1.16689
26	0	1.30539	3.03357	1.16643
27	0	1.17485	3.03395	1.16605
28	4	1.45737	3.03425	1.16575
29	0	1.31163	3.03449	1.16551
30	0	1.18047	3.03469	1.16531
31	1	1.16242	3.03485	1.16515
32	1	1.14618	3.03498	1.16502
33	0	1.03156	3.03508	1.16492
34	1	1.02840	3.03517	1.16483
35	1	1.02556	3.03524	1.16476
36	1	1.02301	3.03529	1.16471
37	1	1.02071	3.03534	1.16466
38	0	0.91864	3.03537	1.16463
39	0	0.82677	3.03540	1.16460
40	1	0.84409	3.03543	1.16457
41	0	0.75969	3.03545	1.16455
42	0	0.68372	3.03546	1.16454
43	0	0.61535	3.03547	1.16453
44	2	0.75381	3.03548	1.16452
45	2	0.87843	3.03549	1.16451
46	2	0.99059	3.03550	1.16450
47	3	1.19153	3.03550	1.16450
48	3	1.37238	3.03551	1.16449
49	0	1.23514	3.03551	1.16449
50	7	1.81162	3.03552	1.16448

Sample	Subgroup value (Z)	EWMA Chart point (Z)	UCL	LCL
51	3	1.93046	3.03552	1.16448
52	1	1.83742	3.03552	1.16448
53	1	1.75367	3.03552	1.16448
54	1	1.67831	3.03552	1.16448
55	0	1.51048	3.03552	1.16448
56	2	1.55943	3.03552	1.16448
57	3	1.70349	3.03553	1.16447
58	3	1.83314	3.03553	1.16447
59	1	1.74982	3.03553	1.16447
60	2	1.77484	3.03553	1.16447
61	3	1.89736	3.03553	1.16447
62	3	2.00762	3.03553	1.16447
63	2	2.00686	3.03553	1.16447
64	2	2.00617	3.03553	1.16447
65	2	2.00556	3.03553	1.16447
66	7	2.50500	3.03553	1.16447
67	3	2.55450	3.03553	1.16447
68	3	2.59905	3.03553	1.16447
69	3	2.63915	3.03553	1.16447
70	1	2.47523	3.03553	1.16447
71	4	2.62771	3.03553	1.16447
72	2	2.56494	3.03553	1.16447
73	2	2.50844	3.03553	1.16447
74	2	2.45760	3.03553	1.16447
75	2	2.41184	3.03553	1.16447
76	3	2.47066	3.03553	1.16447
77	0	2.22359	3.03553	1.16447
78	2	2.20123	3.03553	1.16447
79	2	2.18111	3.03553	1.16447
80	3	2.26300	3.03553	1.16447
81	0	2.03670	3.03553	1.16447
82	0	1.83303	3.03553	1.16447
83	0	1.64972	3.03553	1.16447
84	1	1.58475	3.03553	1.16447
85	1	1.52628	3.03553	1.16447
86	2	1.57365	3.03553	1.16447
87	2	1.61628	3.03553	1.16447
88	2	1.65466	3.03553	1.16447
89	4	1.88919	3.03553	1.16447
90	3	2.00027	3.03553	1.16447
91	3	2.10024	3.03553	1.16447
92	0	1.89022	3.03553	1.16447
93	4	2.10120	3.03553	1.16447
94	4	2.29108	3.03553	1.16447
95	1	2.16197	3.03553	1.16447
96	0	1.94577	3.03553	1.16447
97	0	1.75120	3.03553	1.16447
98	0	1.57608	3.03553	1.16447
99	0	1.41847	3.03553	1.16447
100	0	1.27662	3.03553	1.16447

APPENDIX H

Preliminary Hazard Analysis for the KSC Project

Hazardous Conditions	Hazard Cause	Hazard Effect	Safety/ Engineering Requirements	Hazard Elimination Control Provisions
1. Non-hazard proof electrical equipment	Human Error (Failure to follow SOP)	Fire/Explosion resulting in injury or death to personal and loss of or damage to flight hardware, Ground Support Equipment (GSE), and facility.	Lock out and tag out all non-hazard proof non-electrical equipment	High Pressure Gas Tanks test work authorization procedures (WAP) contain steps requiring a walk down to verify that all electrical equipment has been locked out and tagged.
2. Hose rupture of GSE leak.	Manufacturer defect/hose life	Fire/Explosion resulting in injury or death to personal and loss of or damage to flight hardware, GSE, and facility.	Meet minimum calibration requirements as specified by the manufacturer.	Valid proof test and calibration certification shall be verified prior to hazard operations. WADs shall contain steps that verify that the proof test and calibrations are current.
3. Adiabatic Compression/Overt temp	Human Error (Failure to follow OMSRD Requirements)	Fire/Explosion resulting in injury or death to personal and loss of or damage to flight hardware, GSE, and facility.	Meet OMSRD requirements define the pressurization/depressurization rates	Limit pressurization/depressurization at 50 psi/sec. The addition of an orifice restricting the flow rate of the Pressure Regulating Unit Assembly (PRUA). Monitor and control tank temperatures during fill operations keeping temp. below 115 F. Incorporate monitoring requirements into WAD.
4. Accelerated Particle velocity/cleanliness	Design Deficiency	Fire/Explosion resulting in injury or death to personal and loss of or damage to flight hardware, GSE, and facility.	PRUA cleaned to level 100A per KSC-SPEC-C-123.	Addition of three 10-micron filters one in the inlet side of the PRUA, one is internal to the PRUA and one connected to the HPGTs inlet supply valve. Samples will be taken to verify oxygen cleanliness prior to and after HPGTs servicing.

Hazardous Conditions	Hazard Cause	Hazard Effect	Safety/ Engineering Requirements	Hazard Elimination Control Provisions
5. Structural Failure	Manufacturer defect	Rupture/Damage of High Pressure Gas Tanks (HPGTs) could result in injury or death to personnel and loss of or damage to flight hardware, GSE, and facility.	Meet minimum calibration requirements as specified by the manufacturer.	Perform receiving inspection on the tanks upon arrival at KSC prior to testing to verify tank integrity. Review of receiving inspection and test WADs to verify no damage occurred prior to arrival at KSC.
6. Over pressurization of PRUA	Human Error (Failure to follow SOP)	Damage to PRUA could result in injury or death to personnel and loss of or damage to flight hardware, GSE, and facility.	Design of SOP to meet applicable NASA operational and safety requirements.	No critical failure points or failure modes have been identified in Systems Assurance Analyses that would result in over pressurization of GSE. In the event of a failure, personnel will be in position to turn off the gas supply valve. Train personnel in the hazards related to high-pressure gas systems. Utilize a remote control valve at the gas supply.
7. Failure of crane or lifting support equipment.	Human Error (Failure to follow SOP)	Possible damage or rupture of a HPGTs. Resulting in injury/death to personnel and loss of or damage to flight hardware, GSE, and facility.	Certification of cranes and lifting equipment in accordance to NSS/GO 1740.9. In addition, load tested and operational tested and certified.	Perform walk downs, inspections and functional test prior to operation.

Hazardous Conditions	Hazard Cause	Hazard Effect	Safety/ Engineering Requirements	Hazard Elimination Control Provisions
8. Impact with other structures.	Human Error (Failure to follow SOP)	Possible damage or rupture of a HPGT. Resulting in injury/death to personnel and loss of or damage to flight hardware, GSE, and facility.	If crane is at a distant greater than 10 inches from a structure operation speed has to be less than 2 in./min. Within 10-in. operate less than 1 in./min.	Operators will possess a valid operator's license, which is verified in the WAD. Perform a pre-test briefing shall be held prior to lifting operations and personnel will be advised of their specific task and the hazards involved. A controlled area shall be established for all lifting operations and cleared of all nonessential personnel.

APPENDIX I

Failure Mode and Effect Analysis for the KSC Project

Item/Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Potential Cause(s)/Mechanism(s) of Failure	Current Design Controls	Recommended Action(s)
Tubing / Transport Oxygen from PRUA to HPGT	Ignition	Fire/Explosion resulting in injury or death to personal and loss of or damage to flight hardware, Ground Support Equipment (GSE), and facility.	Striking a valve body just downstream of the control element of the valve can cause Particulate Impact ignition caused by the exposure of un-oxidized metal surfaces.	Five 10 Micron filters remove particulates.	Continue to use five 10 Micron filters remove particulates.
Non-hazard proof electrical equipment / No function	Electrical arcing	Fire/Explosion resulting in injury or death to personal and loss of or damage to flight hardware, Ground Support Equipment (GSE), and facility.	Short circuit and arc through its sheath to the oxygen gas. Human Error (Failure to follow SOP).	Lock out and tag out all non-hazard proof non-electrical equipment.	High Pressure Gas Tanks test work authorization procedures (WAD) contain steps requiring a walk down to verify that all electrical equipment has been locked out and tagged.
PRUA / Regulate Pressure	Leaks/Fire	Resulting in injury or death to personal and loss of or damage to flight hardware, Ground Support Equipment (GSE), and facility.	Orifices and regulators preclude flow rates. Age of Equipment	Tested with High-pressure oxygen. Designed and certified SSP 500004. The GOX supply source is external to the building and capable of isolation with a remote shut-off valve.	Use a portable O ₂ -monitor system to detect oxygen levels.
Communications during hoisting operations	Improper operations, confusion during anomalies, exacerbating emergencies	Accident resulting in injury to personal and loss of or damage to flight hardware, Ground Support Equipment (GSE).	Human Error (Failure to follow SOP)	System layout allows direct verbal and visual communications. All operators are together, none located remotely. Communications with other O & C will be established.	None

Item/ Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Potential Cause(s)/ Mechanism(s) of Failure	Current Design Controls	Recommended Action(s)
Tube Tank Trailer/Supplies GOX	Leak	Fire/Explosion resulting in injury or death to personnel and loss of or damage to flight hardware, Ground Support Equipment (GSE), and facility.	Orifices and regulators preclude flow rates. Age of Equipment.	The GOX supply source is external to the building and capable of isolation with a remote shut-off valve.	Accept Risk
Crane/ Lifting HPGT's equipment.	Impact with other structures.	Possible damage or rupture of a HPGT's. Resulting in injury/death to personnel and loss of or damage to flight hardware, GSE, and facility.	Human Error (Failure to follow SOP)	If crane is at a distant greater than 10 inches from a structure operation speed has to be less than 2 in./min. Within 10-in. operate less than 1 in./min.	Operators will possess a valid operator's license, which is verified in the WAD. Perform a pre-test briefing shall be held prior to lifting operations and personnel will be advised of their specific task and the hazards involved. A controlled area shall be established for all lifting operations and cleared of all nonessential personnel. Certification of cranes and lifting equipment in accordance to NSS/GO 1740.9. In addition, load tested and operational tested and certified.

Item/ Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Potential Cause(s)/ Mechanism(s) of Failure	Current Design Controls	Recommended Action(s)
HPGT/Store Oxygen	Fire	Resulting in injury or death to personnel and loss of or damage to flight hardware, GSE, and facility.	Overtemp due to high pressurization rates. Worst case pressure/flows misunderstood and inadequately addressed. Calibration of measurement systems.	Pressurization rates describe of 40 ft/sec well below the WTSF recommended threshold of 150 ft/sec for stainless steel. Pressurization Rates preclude over-temp. Procedure defines "slow openings" at the valves and regulators.	Limit pressurization/depressurization at 50 psi/sec. The addition of an orifice restricting the flow rate of the Pressure Regulating Unit Assembly (PRUA). Monitor and control tank temperatures during fill operations keeping temp below 115 F. Incorporate monitoring requirements into WAD.
HPGT/ Store Oxygen	Under-pressurization	Mission Failure	Calibration of measurement systems.	All systems are controlled by SPP-M-05, repeatable maintenance recall systems/calibration support.	Inspect calibration stickers during final walk down.
HPGT/ Store Oxygen	Rupture	Rupture/Damage of High Pressure Gas Tanks (HPGT's) could result in injury or death to personnel and loss of or damage to flight hardware, GSE, and facility.	Overpressure	Concrete block walls and housing further shield other flight hardware from this overpressure. Pressurization rates describe of 40 ft/sec well below the WTSF recommended threshold of 150 ft/sec for stainless steel.	Accept Risk

Item/ Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Potential Cause(s)/ Mechanism(s) of Failure	Current Design Controls	Recommended Action(s)
HPGT/Store Oxygen	Ignition	Fire/Explosion resulting in injury or death to personal and loss of or damage to flight hardware, Ground Support Equipment (GSE), and facility.	Adiabatic Compression Release of mechanical strain energy.	Orifices and regulators preclude flow rates, which cause adiabatic compression. Concrete block walls and housing further shield other flight hardware from this overpressure	Continue to use Orifices and regulators preclude flow rates, which cause adiabatic compression. Pressure relief valves set at 110% max fill pressure. Valid proof test and calibration certification shall be verified prior to hazard operations. WADs shall contain steps that verify that the proof test and calibrations are current.
HPGT/ Store Oxygen	Pneumatic Impact	Fire/Explosion resulting in injury or death to personal and loss of or damage to flight hardware, Ground Support Equipment (GSE), and facility.	Heat is generated from the conversion of mechanical work when a gas is compressed from a low to a high pressure.	Pressurization rates describe of 40 ft/sec well below the WTSF recommended threshold of 150 ft/sec for stainless steel.	Addition of three 10-micron filters one in the inlet side of the PRUA, one is internal to the PRUA and one connected to the HPGT's inlet supply valve. Samples will be taken to verify oxygen cleanliness prior to and after HPGT's servicing.

Item/ Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Potential Cause(s)/ Mechanism(s) of Failure	Current Design Controls	Recommended Action(s)
HPGT/Store Oxygen	Ignition by mechanical impact	Fire/Explosion resulting in injury or death to personal and loss of or damage to flight hardware, Ground Support Equipment (GSE), and facility.	It has been determined for several aluminum alloys that the minimum energy to induce sample fracture was less than or equal to the minimum energy required to induce ignitions by mechanical impact. Mechanical impact testing of contaminated surfaces in oxygen indicates an increase in mechanical impact sensitivity (Springer, 1975).	System layout allows direct verbal and visual communications. All operators are together, none located remotely. Communications with other O & C will be established	If crane is at a distant greater than 10 inches from a structure operation speed has to be less than 2 in./min. Within 10-in. operate less than 1 in./min.

APPENDIX J

Barrier Analysis for the KSC Project

Steel Barriers

Barrier Description	Barrier Classification	Type of Failure
All personnel exposed to GOX leaks shall remain isolated from ignition sources for at least 30 min.	Human Barrier	Human Failure
Tube-bank operator shall wear face shield and antistatic clothing while operating valves.	Human Barrier	Technical Failure
All hose connections leak checked prior to usage.	Human Barrier	Technical Failure
Constantly monitoring pressure and temperature during servicing operations.	Technical Barrier	Technical Failure
Visually monitoring pressure and temperature during filling operations.	Human Barrier	Technical Failure
Supervising the proper performance of the Standard Operating Procedures (SOPs).	Human Barrier	Human Failure
Walk downs, inspections and functional tests prior the hoisting/lifting of the HPGTs.	Human Barrier	Technical Failure

Paper Barriers

Barrier Description	Barrier Classification	Type of Failure
All emergency lightning, exits signs, alarm bells, etc. within the control areas are required to remain active during hazardous operations.	Technical Barrier	Technical Failure
All personnel supporting hazardous oxygen operations shall be trained on the hazards involved in the operations and the proper handling of oxygen.	Human Barrier	Human/ Technical Failure
The Center Materials Representative for oxygen compatibility shall approve all materials used in conjunction with oxygen.	Technical Barrier	Technical Failure
A 10-foot control area shall be established around the stored pressurized tanks.	Organizational Barrier	Technical Failure

APPENDIX K

Classification of Dendritics for the KSC Project

Class A Dendritic	Class B Dendritic	Class C Dendritic	Class D Dendritic
Failure to Adhere to Standard Operating Procedure (SOP).	Reaching to Hoist HPGT.	Hose/tubing located in high-traffic area.	Personnel not wearing proper Personal Protective Equipment (PPE).
Protective coverings askew/leaking/corroded.	Operators engaging in practices that divert their attention while operating a Hoist.	Misreading of portable oxygen monitor.	Personnel limitation for a test cell exceeded.
Personnel located under suspended or moving loads.	Instrumentation calibration not done on regular scheduled intervals.	Discrepancies in gauge readings.	
Over pressurization of HPGTs.	Under pressurization of HPGTs.	Spacing from such structures is less than 1 foot preventing maintenance.	
Temperature exceeds preset limits.	Flow rates exceed preset limits.	Abnormal noise.	
Impact of structures with tanks.	General cleanliness.	Unauthorized personnel.	
Malfunctions in compressor and pump resulting in ignition and fire.	Contaminants in oxygen tank components.	Failure to establish safety zones with appropriate barriers (rope, cones, etc.) prior to lift.	
Test being conducted less than 3 m (10 ft) from any opening in walls of adjacent structures.	Excessive vibration of ground support equipment.	Operator not securing area making sure that the area is clear of personnel before starting a hoist.	
Testing being conducted twenty-five feet from any structures with fire-resistive exterior walls or sprinkler buildings of other construction, but not less than one-half the height of adjacent sidewall of the structure.	Full and empty containers stored together.		
Testing being conducted fifty feet from combustible structures.	Incorrect valve operation sequence.		
Test being conducted less than 15.2m (50ft) from solid materials that burn rapidly, such as excelsior or paper.	Releasing GN2 into the O&C.		

Class A Dendritic	Class B Dendritic	Class C Dendritic	Class D Dendritic
Tanks not tested in an adequately vented building.	Introduction of a non-hazard proof electrical equipment.		
Testing in a building of noncombustible construction.	Failure of crane or lifting support equipment.		
Leak checks not performed or performed incorrectly.	Crane inspections not conducted prior to first use each day.		
Oxygen tanks not stored above ground.	Sudden start or stop of crane causing the load to swing out of radii at which it can be controlled.		
Failure to check calibration stickers of measurement equipment.	Hook not centered over the load to prevent swinging.		
Not opening valves and regulators as stated in operation procedures "open slowly".	Multiple parts of the rope are twisted around each other.		
Exposure of oxidized metal surface.	Hoist rope is kinked before starting to hoist.		
Tanks not secured during transportation.	Miscommunication of hand signals.		
Pressure/flows misunderstood and inadequately addressed.	An operator not on hoist controls at times while a load is suspended.		
Tank impact with other structures.	Decalibration of measurement systems.		
Failure to perform all hoist functions in an unloaded condition.			
Crane brake failure.			
Operator continuing operation after communication loss.			
Operator not examining the hoists tag(s) and/or appropriate documentation to ensuring that the hoist is within inspection and periodic certification intervals.			
Uncertified personal using an installed, fixed air, or electric powered hoists systems.			

APPENDIX L

c Control Chart Data for the KSC Project

Subgroup or sample	Number of dendritics in observation h of sample i				Total number of dendritics in sample i
	1	2	3	4	
1	1	1	1	1	4
2	1	1	1	1	4
3	1	1	1	0	3
4	1	0	0	0	1
5	0	1	0	0	1
6	0	0	0	0	0
7	0	1	0	0	1
8	0	0	0	2	2
9	2	0	1	2	5
10	0	2	2	1	5
11	2	0	1	2	5
12	1	1	1	0	3
13	1	1	0	2	4
14	2	1	1	0	4
15	1	1	0	0	2
16	1	0	0	0	1
17	1	0	0	1	2
18	0	0	1	1	2

APPENDIX M

Weighted Control Chart Data for the KSC Project

Sample	Class A	Class B	Class C	Class D	D_i	n_i	\bar{u}_A	\bar{u}_B	\bar{u}_C	\bar{u}_D
1	0	0	4	0	40	10.00	0.00	0.00	1.00	0.00
2	0	0	4	0	40	10.00	0.00	0.00	1.00	0.00
3	0	0	3	0	30	7.50	0.00	0.00	0.75	0.00
4	1	0	0	0	100	25.00	0.25	0.00	0.00	0.00
Preliminary Sampling Study							\bar{u}_A	\bar{u}_B	\bar{u}_C	\bar{u}_D
							0.0625	0.00	0.6875	0.00
Sample	Class A	Class B	Class C	Class D	D_i	n_i	\bar{u}_A	\bar{u}_B	\bar{u}_C	\bar{u}_D
5	0	1	0	0	50	12.50	0.00	0.25	0.00	0.00
6	0	0	0	0	0	0.00	0.00	0.00	0.00	0.00
7	0	0	0	1	1	0.25	0.00	0.00	0.00	0.25
8	0	1	0	1	51	12.75	0.00	0.25	0.00	0.25
9	1	1	0	3	153	38.25	0.25	0.25	0.00	0.75
10	0	0	2	3	23	5.75	0.00	0.00	0.50	0.75
11	1	3	0	1	251	62.75	0.25	0.75	0.00	0.25
12	0	2	0	1	101	25.25	0.00	0.50	0.00	0.25
13	1	2	0	1	201	50.25	0.25	0.50	0.00	0.25
14	0	1	0	3	53	13.25	0.00	0.25	0.00	0.75
15	0	0	0	2	2	0.50	0.00	0.00	0.00	0.50
16	1	0	0	0	100	25.00	0.25	0.00	0.00	0.00
17	2	0	0	0	200	50.00	0.50	0.00	0.00	0.00
18	2	0	0	0	200	50.00	0.50	0.00	0.00	0.00